

IN THE SUPERIOR COURT OF FORSYTH COUNTY
STATE OF GEORGIA


Greg G. Allen, Clerk
Forsyth County, Georgia

Linda Louise Denwood, Carlos Capriles,
Allyson Snider and Andrew DeBate,

Plaintiffs,

v.

Peachtree Orthopaedic Clinic, P.A.,

Defendant.

File No. 23-CV-1234-3

JURY TRIAL DEMANDED

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Linda Louise Denwood, Carlos Capriles, Allyson Snider, and Andrew DeBate (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, for their Consolidated Class Action Complaint, bring this action against Defendant Peachtree Orthopedic Clinic, P.A. (“Peachtree” or “Defendant”) based on personal knowledge and the investigation of counsel and allege as follows:

INTRODUCTION

1. Between April 14, 2023 and April 20, 2023, an unknown actor gained unauthorized access to Peachtree’s inadequately protected computer systems. As a result, Plaintiffs and the Class Members (as further defined below) have had their personal identifiable information¹ (“PII”), personal health information (“PHI”), and financial account information (collectively, “Private Information”) exposed (the “Data Breach”).

2. Peachtree is a medical group providing orthopedic care in the Atlanta area.²

¹ Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

² See *Why Choose Us*, Peachtree Orthopedics, <https://peachtreeorthopedics.com/about-us/> (last accessed July 21, 2023).

3. Peachtree provides medical services to thousands of patients every year.
4. Plaintiffs and the Class Members are current and former patients of hospitals or physician centers owned by Defendant or one of its parents or affiliates.
5. In order to receive medical services, Plaintiffs and Class Members were required to provide Defendant with their Private Information and did so with the understanding that such information would be kept safe from unauthorized access.
6. By taking possession and control of Plaintiffs' and Class Members' Private Information, Defendant assumed a duty to securely store and protect their Private Information.
7. The Data Breach was discovered on April 20, 2023, when Defendant noticed suspicious activity on its computer network. Defendant investigated the attack with the assistance of third-party specialists and confirmed that an unauthorized party had gained access to certain files on Defendant's network between April 14, 2023 and April 20, 2023.
8. According to Peachtree, the Private Information exposed to and potentially accessed or acquired by cybercriminals includes names, addresses, dates of birth, driver's license numbers, Social Security numbers, medical treatment and diagnosis information, treatment costs, financial account information, health insurance claims, and health insurance provider information.
9. Although Defendant is a sophisticated medical entity providing services to thousands of patients, Defendant failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and medical information of approximately 34,691 individuals, including Plaintiffs and Class Members.³ As a direct, proximate, and

³ *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed July 21, 2023); see Steve Adler, *Peachtree Orthopedics Suffers Data Theft and Extortion Incident*, THE HIPAA JOURNAL (June 8, 2023), <https://www.hipaajournal.com/peachtree-orthopedics-suffers-data-theft-and-extortion-incident/>.

foreseeable result of Defendant's failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised Defendant's network and accessed thousands of patient files containing highly-sensitive Private Information.⁴

10. Around July 2023, Peachtree began notifying Plaintiffs and Class Members of the Data Breach.

11. Due to Defendant's negligence, cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of Plaintiffs and the Class.

12. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the Private Information of approximately 34,691 individuals that was exposed in a major data breach of Peachtree's network in violation of its legal obligations.⁵

13. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiffs and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

14. Defendant betrayed the trust of Plaintiffs and the other Class Members by failing to properly safeguard and protect their Private Information and thereby enabling cybercriminals to steal such valuable and sensitive information.

⁴ *Id.*

⁵ *Id.*

15. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies that this Court deems necessary and proper.

THE PARTIES

16. Plaintiff Linda Louise Denwood is a resident and citizen of Marietta, Georgia. Plaintiff Denwood received a data breach letter from Defendant in mid-July 2023.

17. Plaintiff Carlos Capriles is a resident and citizen of Buford, Georgia. Plaintiff Capriles received a data breach letter from Defendant in mid-July 2023.

18. Plaintiff Allyson Snider is a resident and citizen of Atlanta, Georgia. Plaintiff Snider received a data breach letter from Defendant in mid-July 2023.

19. Plaintiff Andrew DeBate is a resident and citizen of Atlanta, Georgia. Plaintiff DeBate received a data breach letter from Defendant in mid-July 2023.

20. Peachtree is incorporated in Georgia with its principal place of business located at 2860 Ronald Reagan Blvd., Suite 300, Cumming, Georgia, 30041, and is subject to the jurisdiction of this court.

21. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

22. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction pursuant to GA Code § 15-6-8.

24. Defendant is a citizen of Georgia because it is incorporated in Georgia with its principal place of business in Cumming, Georgia.

25. This Court has personal jurisdiction over Defendant because it conducts substantial business in Georgia and this District and collected and/or stored the Private Information belonging Plaintiffs and Class Members in this District.

26. Venue is proper in this Court because Defendant's principal office is in this county, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this county. *See* GA. CODE § 14-2-510(b).

FACTUAL ALLEGATIONS

Background

27. Defendant is a medical practitioner group that provides orthopedic health care services.⁶ Defendant represents to its patients that, “[w]ith Peachtree Orthopedics, you’re set for life,” because “it really is about you, and we want you to get back to life and to doing the things you love – without fear or pain – as fast as possible.”⁷

28. As part of its medical and business operations, Defendant required that Plaintiffs and Class Members provide their Private Information in order to obtain medical services.

⁶ *Why Choose Us*, Peachtree Orthopedics, <https://peachtreeorthopedics.com/about-us/> (last accessed July 21, 2023).

⁷ *Id.*

29. Current and former patients of Defendant, such as Plaintiffs and Class Members, allowed their Private Information to be made available to Defendant with the reasonable expectation that Defendant would comply with its obligation to keep their sensitive and personal information, including their PII and PHI, confidential and secure from illegal and unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their Private Information.

30. Plaintiffs and Class Members relied on Defendant, a sophisticated medical practice, to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their Private Information.

31. Defendant has a duty to adopt reasonable measures to Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

32. Unfortunately for Plaintiffs and Class Members, Defendant failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security, thus failing to protect Plaintiffs and Class Members from the exfiltration of their Private Information during the Data Breach.

The Data Breach

33. Defendant disclosed in a notice dated July 17, 2023, that between April 14, 2023 and April 20, 2023, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to Defendant's systems and acquired certain files and information, including Plaintiffs' and Class Members' Private Information.

34. The Data Breach was not detected until April 20, 2023. Prior to that time, cybercriminals were able to roam Defendant's systems undetected. *See id.*

35. Upon discovering the Data Breach, Defendant engaged “third-party specialists to determine the full nature and scope of the situation.” Following an investigation, it was determined that an unauthorized party gained access to certain files on Defendant’s network, which contained current and former patients’ names, addresses, dates of birth, driver’s license numbers, Social Security Numbers, medical treatment and diagnosis information, treatment costs, financial account information, and health insurance claims and provider information, including Plaintiffs’ and the Class’s Private Information. *See id.*

36. Defendant admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members. *Id.*

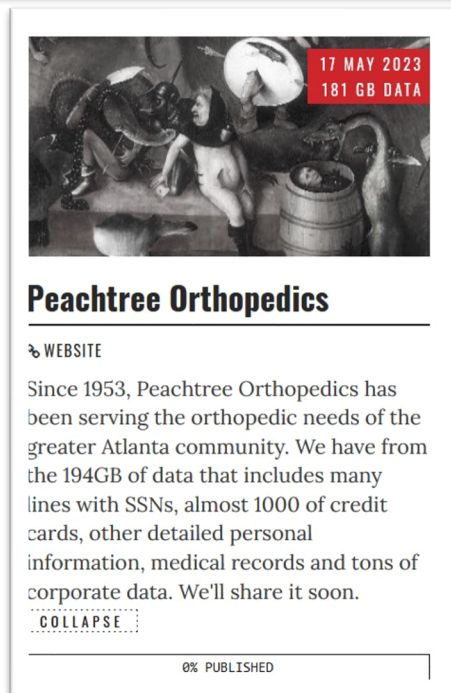
37. During the time that the unauthorized actors had unrestricted access to Defendant’s network, they were able to access and acquire personal, sensitive, and protected Private Information belonging to over 34,691 current and former patients of Defendant.

38. Upon information and belief, the ransomware gang, Karakurt, was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors, Karakurt has perpetrated multiple high-profile breaches in the last two years alone.⁸ Defendant knew or should have known of the tactics that groups like Karakurt employ.

39. With the Private Information secured and stolen by Karakurt, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant has provided no public information on the ransom demand or payment.

⁸ Deep Web Profile, SOCRadar, <https://socradar.io/deep-web-profile-karakurt-extortion-group/#:~:text=Karakurt%20can%20be%20described%20as,variation%20of%20the%20Karakurt%20victims> (last accessed October 24, 2023).

40. On September 14, 2023, the presumed deadline of Karakurt's ransom demand, Karakurt announced it would begin releasing information obtained from the Breach on a data leak page. On information and belief, over 194GB of stolen information, including current and former patients' Social Security numbers, financial information, medical records, and other Private Information were released onto the data leak page.



41. Moreover, despite learning as early as April 20, 2023, that unauthorized actors like Karakurt had accessed its computer systems and confirming that the unauthorized actors accessed and exfiltrated patient Private Information, Defendant delayed sending individualized notice to affected patients until approximately *three months* after it discovered the Data Breach—preventing Plaintiffs and Class members from being able to take steps to protect themselves and their Private Information from misuse.

42. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure another breach does not occur have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

43. The unencrypted Private Information of Plaintiffs and Class Members may end up for sale on the dark web or fall into the hands of third parties that will use the detailed Private Information for unauthorized activities, from identity theft to targeted marketing without the approval of Plaintiffs and Class Members. Due to Defendant's failure to adequately secure its networks, unauthorized individuals can now easily access the Private Information of Plaintiffs and Class Members.

44. Even though protecting Private Information is vital to virtually every aspect of Defendant's operations as a medical group, Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Plaintiffs' and Class Members' Private Information.

45. The Data Breach also highlights the inadequacies inherent in Defendant's network monitoring procedures. If Defendant had properly monitored its cyber security systems, it would

have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from accessing patients' Private Information.

46. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

47. First, Defendant failed to timely secure its computer systems to protect its current and former patients' Private Information. Defendant allowed the unauthorized actors to continue to have unfettered access to Defendant's systems for an undisclosed period of time until Defendant finally discovered the Data Breach.

48. Second, Defendant failed to timely notify affected individuals, including Plaintiffs and Class Members, that their highly sensitive Private Information had been accessed by unauthorized third parties. Defendant waited approximately three months after discovering the Data Breach to provide notice to the victims of the Data Breach that their Private Information had been compromised.

49. Third, Defendant made no effort to protect Plaintiffs and the Class from the long-term consequences of Defendant's acts and omissions. Defendant's one-year of complimentary credit monitoring and fraud assistance services is inadequate as Plaintiffs' and Class Members' Private Information, including their Social Security numbers, medical information, and financial account information, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiffs and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

50. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and to notify Plaintiffs and Class Members with reasonable timeliness that their Private Information had been accessed due to Defendant's security failures, allowed unauthorized

individuals to access and misappropriate Plaintiffs' and Class Members' Private Information for months before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

51. Because Defendant had a duty to protect Plaintiffs' and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

The Data Breach was Foreseeable

52. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

53. Moreover, Defendant was on notice that companies in the healthcare industry are susceptible targets for data breaches.

54. Defendant was on notice that the FBI has been concerned about data security in the healthcare industry in the years preceding the Data Breach. 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 (PI)."⁹

55. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly

⁹ Finkle, Jim, *FBI Warns Healthcare Firms that They are Targeted by Hackers*, Reuters (Aug. 20, 2014) <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820>.

visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.”¹⁰

56. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”¹¹

57. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”¹²

58. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.¹³ In 2022, the largest growth in compromises occurred in the healthcare sector.¹⁴

59. Healthcare related breaches have continued to rapidly increase because electronic data is seen as a valuable asset. Companies operating within the healthcare industry “have emerged

¹⁰ *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019) available at <https://www.ic3.gov/Media/Y2019/PSA191002> (emphasis added).

¹¹ ZDNet, *Ransomware mentioned in 1,000+ SEC filings over the past year* (Apr. 30, 2020) (emphasis added), available at <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Jan. 25, 2022).

¹² U.S. CISA, *Ransomware Guide – September 2020*, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

¹³ *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, <https://www.idtheftcenter.org/2018-data-breaches/> (last visited Sept. 6, 2023).

¹⁴ *2022 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Sept. 6, 2023).

as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹⁵

60. The American Medical Association (“AMA”) has also warned companies about the importance of protecting 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.¹⁶

61. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its email accounts, databases, servers, and networks and yet it appears Defendant did not encrypt these email accounts, databases, servers, and networks or the information contented within them.

62. The United States Department of Health and Human Services’ (“HHS”) Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the HHS’s Office of Human Rights’ deputy director of health information

¹⁵ *How to Safeguard Hospital Data from Email Spoofing Attacks*, Inside Digital Health (Apr. 4, 2019) <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks>.

¹⁶ 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>.

privacy, stated “[o]ur message to these organizations is simple: encryption is your best defense against these incidents.”¹⁷

63. As a company operating within the healthcare sector, and a covered entity or business associate under HIPAA, Defendant should have known about its data security weaknesses and sought better protection for the Personal Information maintained on its systems and accumulating in its business email accounts.

64. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting health care companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

65. Considering the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information, and Defendant’s type of business had cause to be particularly on guard against such an attack.

66. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs’ and Class Members’ Private Information could be accessed, exfiltrated, and published as the result of a cyberattack.

¹⁷ *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep’t of Health and Human Services (Apr. 22, 2014), available at <https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html>.

67. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

Plaintiffs' Experiences

Plaintiff Linda Denwood's Experience

68. Plaintiff Denwood was a patient at Peachtree in in 2021. She entrusted her Private Information to Defendant in order to receive medical care.

69. Plaintiff Denwood received Defendant's Notice of Data Breach in mid-July, 2023. The Notice stated that Plaintiff Denwood's Private Information, including her address, date of birth, driver's license number, Social Security number, medical treatment/diagnosis information, treatment cost, financial account information, and health insurance claims/provider information, was breached.

70. As a result of the Data Breach, Plaintiff Denwood's sensitive information may have been accessed and/or acquired by an unauthorized actor.

71. The confidentiality of Plaintiff Denwood's sensitive Private Information has been irreparably harmed. For the rests of her life, Plaintiff Denwood will have to worry about when and how her sensitive information may be shared or used to her detriment.

72. As a result of the Data Breach, Plaintiff Denwood spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

73. Additionally, Plaintiff Denwood is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

74. Plaintiff Denwood stores any documents containing her sensitive Private Information in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

75. Plaintiff Denwood suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

76. Plaintiff Denwood has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her Social Security number, financial account information and medical information, being placed in the hands of unauthorized third parties and possibly criminals.

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

Plaintiff Carlos Capriles's Experience

78. Plaintiff Capriles is a patient at Peachtree. He entrusted his Private Information to Defendant in order to receive medical care.

79. Plaintiff Capriles received Defendant's Notice of Data Breach in mid-July, 2023. The Notice stated that Plaintiff Capriles's Private Information, including his name, address, date of birth, driver's license number, Social Security number, medical treatment/diagnosis

information, treatment cost, financial account information, and health insurance claims/provider information, was breached.

80. Plaintiff does not recall ever learning that his Private Information was compromised in a data breach incident, other than the breach at issue in this case.

81. As a result of the Data Breach, Plaintiff Capriles's sensitive information may have been accessed and/or acquired by an unauthorized actor.

82. The confidentiality of Plaintiff Capriles's sensitive Private Information has been irreparably harmed. For the rests of his life, Plaintiff Capriles will have to worry about when and how his sensitive information may be shared or used to his detriment.

83. As a result of the Data Breach, Plaintiff Capriles spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

84. Additionally, Plaintiff Capriles is very careful about not sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

85. Plaintiff Capriles stores any documents containing his sensitive Private Information in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

86. Plaintiff Capriles suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

87. Plaintiff Capriles has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, financial account information and medical information, being placed in the hands of unauthorized third parties and possibly criminals.

88. Indeed, as a result of the Data Breach and in an effort to protect his Private Information from additional exposure, Plaintiff Capriles was forced to purchase and install a security program on his phone for \$5.00/month that he continues to pay for.

89. Additionally, on October 11, 2023, Plaintiff was alerted through Experian that his Social Security trace result, address search result, and dark web search result, all returned with significant risk of exposure, suggesting that his Private Information is in the hands of cybercriminals.

90. Finally, following the Data Breach, Plaintiff Capriles began experiencing an increase of spam calls that identify him through his name, further suggesting that his Private Information is in the hands of cybercriminals.

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

Plaintiff Snider's Experience

92. Plaintiff Snider was a patient at Peachtree. She entrusted her Private Information to Defendant in order to receive medical care.

93. Plaintiff Snider received Defendant's Notice of Data Breach in mid-July, 2023. The Notice stated that Plaintiff Snider's Private Information, including her address, date of birth, Social

Security number, medical treatment/diagnosis information, treatment cost, financial account information, and health insurance claims/provider information, was breached.

94. As a result of the Data Breach, Plaintiff Snider's sensitive information may have been accessed and/or acquired by an unauthorized actor. To date, Plaintiff Snider has experienced issues with unknown persons gaining access to her email account around April-May 2023, the same email that was provided to Peachtree. Plaintiff Snider has spent time resetting her password.

95. The confidentiality of Plaintiff Snider's sensitive Private Information has been irreparably harmed. For the rests of her life, Plaintiff Snider will have to worry about when and how her sensitive information may be shared or used to his detriment.

96. As a result of the Data Breach, Plaintiff Snider spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

97. Additionally, Plaintiff Snider is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

98. Plaintiff Snider stores any documents containing her sensitive Private Information in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

99. Plaintiff Snider suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

100. Plaintiff Snider has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her Social Security number, financial account information and medical information, being placed in the hands of unauthorized third parties and possibly criminals.

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

Plaintiff Andrew DeBate's Experience

102. Plaintiff DeBate is a former patient at Peachtree. He entrusted his Private Information to Defendant in order to receive medical care.

103. Plaintiff DeBate received Defendant's Notice of Data Breach in mid-July, 2023. The Notice stated that Plaintiff DeBate's Private Information, including his name, address, date of birth, driver's license number, Social Security number, medical treatment/diagnosis information, treatment cost, financial account information, and health insurance claims/provider information, was breached.

104. Plaintiff does not recall ever learning that his Private Information was compromised in a data breach incident, other than the breach at issue in this case.

105. As a result of the Data Breach, Plaintiff DeBate's sensitive information may have been accessed and/or acquired by an unauthorized actor.

106. The confidentiality of Plaintiff DeBate's sensitive Private Information has been irreparably harmed. For the rest of his life, Plaintiff DeBate will have to worry about when and how his sensitive information may be shared or used to his detriment.

107. As a result of the Data Breach, Plaintiff DeBate spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

108. Additionally, Plaintiff DeBate is very careful about not sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

109. Plaintiff DeBate stores any documents containing his sensitive Private Information in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

110. Plaintiff DeBate suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

111. Plaintiff DeBate has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, financial account information and medical information, being placed in the hands of unauthorized third parties and possibly criminals.

112. Indeed, Plaintiff already suffered from a flood of identity theft and fraud including:

- a. Version Wireless: On 7/1/2023 Plaintiff received a letter denying his application for a credit card and informing him that he owed \$124.75 for services and \$1,166.55 for an iPhone, none of which Plaintiff applied for or purchased;

- b. SyncB Version: On 5/21/2023, a loan was applied to using Plaintiff's name which was denied;
- c. American Express: On 5/1/2023, Plaintiff received a call from a representative in the American Express fraud department informing him that someone applied to a loan in his name which was denied;
- d. Best Buy: Cybercriminals attempted to apply for a credit card in person using Plaintiff's identity which was denied;
- e. Capital One Auto Finance: On 6/9/2023, cybercriminals applied for a loan using Plaintiff's identity which was denied;
- f. Capital One Bank: On 4/14/2023, someone applied for a loan using Plaintiff's identity which was denied;
- g. Dossett Big Four Buick: On 6/9/2023, someone applied for a loan using Plaintiff's identity which was denied;
- h. Wells Fargo: On 4/22/2023, someone applied for a loan and credit card using Plaintiff's identity which was denied;
- i. Citizens Bank: Cybercriminals used Plaintiff's identity to apply for a loan which was denied;
- j. Ally Financial: Cybercriminals used Plaintiff's identity to apply for a loan; and

- k. Spectrum Cable/Charter Communications: An account that was created under a different name was falsely transferred to Plaintiff's identity. The account's balance is \$4,548.41.

113. Additionally, there were numerous fraudulent hard inquiries on his credit report. In early 2023, Plaintiff's credit score with Experian was over 800 points—but due to these inquiries, Plaintiff's credit score dropped to 666 on November 10, 2023. The fraudulent credit inquiries include:

- a. Version Wireless;
- b. SyncB Version;
- c. American Express;
- d. Best Buy;
- e. Capital One Auto Finance;
- f. Capital One Bank;
- g. Dossett Big Four Buick;
- h. Wells Fargo;
- i. Citizens Bank; and
- j. Ally Financial.

114. Plaintiff also suffered from medical fraud and identity theft. The following charges were billed to his health insurance (however, he never received such services himself):

- a. Grady EMS on 9/3/2023 for \$1,919.50;
- b. Emory St. Joseph's Hospital on 9/3/2023 for \$1,958.79; and
- c. Emory Employer on 9/4/2023 for \$68.

115. Finally, following the Data Breach, Plaintiff DeBate began experiencing an increase of spam calls and texts, further suggesting that his Private Information is in the hands of cybercriminals.

116. In the aftermath of the Data Breach—and the flood of fraud and identity theft that followed—Plaintiff spent approximately 500 hours attempting to mitigate the damages. This time was spent on:

- a. calling the fraud departments of agencies that made inquiries on his credit report;
- b. calling the police non-emergency number to speak with officers;
- c. driving to different precincts to speak with police officers and ask for help;
- d. filing (and paying to file) a police report;
- e. petitioning the City of Atlanta to assign him an investigator which included traveling to Atlanta (about an hour away) and paying for parking;
- f. working with the investigator to obtain more information about the application made in the Best Buy store;
- g. traveling to the DMV and paying for a new license and license number;
- h. calling Social Security for help;
- i. filing a report with the FTC;

- j. signing up for LifeLock which included an extensive application detailing all of the fraud he experienced;
- k. for each of the hard inquiries on his credit report, Plaintiff spent time calling the companies, filing a report, having the report notarized and sent through certified mail;
- l. filing and notarizing reports for each of the three credit bureaus;
- m. calling many different government agencies multiple times including the OIG fraud hotline;
- n. calling each of the three credit bureaus many times;
- o. freezing his credit with each of the three bureaus; and
- p. taking a week off from work to address the fraud.

117. In total, Plaintiff incurred *at least* \$1,000 in costs spent trying to mitigate the fraud (without including the value of his lost time and opportunity costs from missing work).

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

Defendant Had Duties to Secure the Private Information and Prevent the Breach

119. Defendant acquired, collected, and stored the Private Information of Plaintiffs and Class Members.

120. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

121. Plaintiffs and other Members of the Class entrusted their highly sensitive Private Information to Defendant.

122. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

123. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and obligations and knew or should have known that it was responsible for protecting the Private Information from disclosure.

124. Defendant's obligations are derived from: 1) government regulations and state laws, including HIPAA and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive Private Information. Plaintiffs and Class Members provided, and Defendant obtained, their Private Information on the understanding that their Private Information would be protected and safeguarded from unauthorized access or disclosure.

125. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁸

126. 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.

¹⁸ See *How to Protect Your Networks from RANSOMWARE*, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ciso.pdf/view> (last visited July 17, 2023).

- 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.¹⁹

127. 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 Cybersecurity & Infrastructure Security Agency, 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. . . .
- **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

¹⁹ *Id.* at 3-4.

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 traffic²⁰

128. 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 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

²⁰ See *Security Tip (ST19-001) Protecting Against Ransomware* (original release date Apr. 11, 2019), available at <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited July 17, 2023).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²¹

129. Given that Defendant was storing the Private Information of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

130. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

131. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet- accessible environment when there was a reasonable need to do so.

132. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

133. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

134. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen,

²¹ See *Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Failed to Adhere to FTC Guidelines

135. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of personal information—including Social Security numbers and financial account information—that identifies customers or employees.

136. Additionally, the FTC’s Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

137. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²³

138. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. Protect the sensitive consumer information that they keep;

²² 17 C.F.R. § 248.201 (2013).

²³ *Id.*

- b. Properly dispose of PII that is no longer needed;
- c. Encrypt information stored on computer networks;
- d. Understand their network's vulnerabilities; and
- e. Implement policies to correct security problems.

139. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

141. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

142. Defendant knew or should have known these rules and guidelines and the importance of adhering to them.

143. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class's Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Failed to Adhere to HIPAA Guidelines

144. Upon information and belief, Defendant is covered by HIPAA (45C.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.

145. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”). *See* 42 U.S.C. § 17921; 45 C.F.R. § 106.103. HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

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

147. 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, including health information that is kept or transferred in electronic form.

148. 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.

149. “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.

150. 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.

151. 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).

152. Additionally, HIPAA 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).

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

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

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

156. HIPAA also requires the Office of Civil Rights (“OCR”), within HHS, to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- PHI and comply with the risk analysis requirements of the Security Rule.”²⁴ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.”²⁵

157. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”

158. Defendant knew or should have known these rules and guidelines and the importance of adhering to them.

²⁴ US Department of Health & Human Services, Security Rule Guidance Material, <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

²⁵ US Department of Health & Human Services, Guidance on Risk Analysis, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed July 11, 2023).

159. Upon information and belief, Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiffs and the Class from unauthorized access and disclosure.

160. Upon information and belief, Defendant's security failures include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR § 164.306(a)(1);
- d. 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 CFR § 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR § 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR § 164.308(a)(6)(ii);

- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR § 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR § 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR § 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR §§ 164.502, *et seq.*

161. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

162. Defendant also violated the HIPAA Breach Notification Rule since it did not inform Plaintiffs and the Class members about the breach until **88 days** after it first discovered the breach.

163. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class's Private Information constitutes an unfair act or practice prohibited by HIPAA.

164. Because Defendant has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security is adequate and appropriate going forward.

Defendant still maintains the PHI and other highly sensitive PII of its current and former customers and employees, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

Defendant Failed to Adhere to Industry Standards

165. As noted above, healthcare businesses are routinely identified as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

166. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Defendant include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

167. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

168. Defendant should have also followed the minimum standards of any one 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.

169. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant's Response to the Data Breach is Inadequate

170. Defendant purports to care about data security and safeguarding patients' Private Information and represents that it will keep secure and confidential the Private Information belonging to its current and former patients.

171. Plaintiffs' and Class Members' Private Information was provided to Defendant in reliance on its promises and self-imposed obligations to keep Private Information confidential, and to secure the Private Information from unauthorized access by malevolent actors. Defendant failed to do so.

172. Defendant was negligent and failed to inform Plaintiffs and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

173. Defendant admitted that it learned of the data breach as early as April 20, 2023. Yet, Defendant did not start notifying affected individuals until months later, on or around mid-July 2023.

174. During these intervals, the cybercriminals have had the opportunity to exploit Plaintiffs' and the Class Member's Private information while Defendant was secretly investigating the Data Breach.

175. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with just a single year of credit

monitoring through Kroll. However, this is much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendant's failures.

Value of Private Information

176. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁶ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁸

177. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

178. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."²⁹

²⁶ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

²⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²⁸ *In the Dark*, VPNOverview (2019) available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

²⁹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack->

179. Health insurance information can be used to steal someone’s medical identity.³⁰ Once someone’s medical identity has been stolen, the information can be used to fraudulently obtain medical care or submit fraudulent claims for payment to health insurers without your authorization.³¹ This type of identity theft can lead to unauthorized charges on a patient’s account, incorrect reporting of a patient’s medical record, and a diminished level of medical services.

180. 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.³²

181. Almost 50 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.³³

182. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

personal-data- stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

³⁰ U.S. Dep’t of Veterans Affairs Office of Inspector General & Federal Bureau of Investigation, FRAUD ALERT Medical Identity Theft, [chrome-extension://efaidnbmninnibpcjpcglclefindmkaj/https://www.va.gov/oig/fraud/Medical_Identity_Theft.pdf](https://www.va.gov/oig/fraud/Medical_Identity_Theft.pdf) (last visited on Sept. 5, 2023).

³¹ *Id.*

³² Mills, Elinor, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last visited Sept. 6, 2023).

³³ *Id.*

183. One such example of criminals using Private Information for profit is the development of “Fullz” packages.

184. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

185. The development of “Fullz” packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and the Class’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

186. That is exactly what is happening to Plaintiffs and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs’ and the Class’s stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

Plaintiffs and the Class Face Significant Risk of Continued Identity Theft

187. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, “Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come.”³⁴

³⁴ Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: <http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers>.

188. The FTC warns the public to pay particular attention to how they keep personally identifying information, including Social Security numbers and other sensitive data. As the FTC notes, “once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”³⁵

189. The ramifications of Defendant’s failure to properly secure Private Information, including Plaintiffs’ and Class Members’ Social Security Numbers, medical records, and financial account information, are severe. Identity theft occurs when someone uses another person’s financial and personal information, such as that person’s name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

190. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

191. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, they can be used in more ways than one, and it typically takes time for an information breach to be detected.

192. Accordingly, Plaintiffs and members of the proposed Class have suffered injury and/or will likely suffer injury from the misuse of their Private Information that can be directly traced to Defendant.

193. Defendant negligently disclosed the Private Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiffs and the Class to people engaged in

³⁵ *Warning Signs of Identity Theft*, FEDERAL TRADE COMM’N, available at: <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed Apr. 5, 2023).

disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen Private Information.

194. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with one year of credit monitoring. However, one year of complimentary credit monitoring is a time frame much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class Members by Defendant's failures.

195. Moreover, the credit monitoring offered by Defendant is inadequate to protect Plaintiffs and Class Members from the injuries resulting from the unauthorized access of their sensitive Private Information.

196. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their Private Information is used;
- b. The diminution in value of their Private Information;
- c. The compromise and continuing publication of their Private Information;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including, but not limited to, efforts spend researching how to prevent, detect, contest, and recover from identity theft and fraud;

- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Private Information; and
- h. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in their possession.

197. The fraudulent activity resulting from the Data Breach may not come to light for years.

198. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used, and the risk will not abate within a year. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³⁶

199. Defendant's negligence and failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach

³⁶ Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>.

200. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

201. Plaintiffs retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

202. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

203. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers and medical information, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

204. The injuries to Plaintiffs and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

V. CLASS ACTION ALLEGATIONS

205. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Ga. Code Ann., § 9-11-23.

206. The Class that Plaintiffs seek to represent is defined as follows:

All individuals whose Private Information may have been accessed and/or acquired in the ransomware attack that is the subject of the Notice of Data Breach

that Defendant sent to Plaintiffs and Class Members on or around July 17, 2023 (the “Class”).

207. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

208. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

209. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process, Defendant reported to the Maine Attorney General that 34,691 individuals were impacted by the Data Breach. The members of the Class will be identifiable through information and records in Defendant’s possession custody, and control.

210. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

- c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant's computer systems and data security used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act, HIPAA, and/or state laws and/or Defendant's other duties discussed herein;
- j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- k. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to safeguard the Private Information of Plaintiffs and Class Members;
- l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

- n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

211. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiffs and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

212. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

213. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

214. **Superiority and Manageability:** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum

simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

215. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

216. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

217. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

218. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

219. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Ga. Code Ann., § 9-11-23(b)(2).

220. Likewise, particular issues under Ga. Code Ann., § 9-11-23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- f. Whether Defendant's computer systems and data security used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act, HIPAA, and/or state laws and/or Defendant's other duties discussed herein;
- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,
- h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

221. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

222. Defendant solicited, gathered, and stored the Private Information of Plaintiffs and the Class as part of the operation of its business.

223. Upon accepting and storing the Private Information of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

224. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

225. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

226. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive Private Information.

227. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

228. Defendant's duty extended to protecting Plaintiffs 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.

229. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common- sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs 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 Plaintiffs' and Class Members' Private Information was adequately secured from impermissible access, viewing, release, disclosure, and publication;
- b. To protect Plaintiffs' and Class Members' Private Information in its 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 networks and servers; and
- d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

230. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

231. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;
- b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. Failing to adequately train its employees to not store Private Information longer than absolutely necessary;
- d. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Private Information; and
- e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

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

233. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages.

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

235. As a result of the Data Breach, Plaintiffs 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, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

236. As a result of the Data Breach, Plaintiffs and the Class Members have experienced, or will likely experience, unknown persons gaining access to their online accounts, an increase in spam calls, having their information posted on the Dark Web for cybercriminals to access, and having to pay for additional security protections.

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

238. The damages Plaintiffs and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's negligent and/or grossly negligent conduct.

COUNT II – NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

240. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties the FTC Act, HIPAA, common law, and

other state and federal laws. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

241. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII and PHI.

242. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders also form part of the basis of Defendant's duty in this regard.

243. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

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

245. Pursuant to HIPAA, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI.

246. HIPAA requires compliance with its "applicable standards, implementation specifications, and requirements," including, HIPAA's Security Rule. The HIPAA's rules, publications, and orders also form part of the basis of Defendant's duty in this regard.

247. Defendant violated HIPAA by failing to use reasonable measures to protect consumers PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

248. Defendant's violations of Section 5 of the FTC Act and HIPAA constitute negligence *per se* as Defendant's violations of the FTC Act and HIPAA establish the duty and breach elements of negligence.

249. Plaintiffs and Class Members are within the class of persons that the FTC Act and HIPAA are intended to protect.

250. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA are intended to guard against.

251. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

252. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

253. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III – INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

254. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

255. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

256. Defendant owed a duty to Plaintiffs and Class Member to keep their Private Information confidential.

257. Defendant affirmatively and recklessly disclosed Plaintiffs and Class Members' Private Information to unauthorized third parties.

258. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

259. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

260. In failing to protect Plaintiffs' and Class Members' Private Information, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

261. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

262. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

263. As a proximate result of Defendant's acts and omissions, Plaintiffs' and the Class Members' private and sensitive Private Information was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

264. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

265. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiffs' and the Class's Private Information.

266. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information.

267. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

269. By requiring Plaintiffs and the Class Members Private Information as a condition to receiving medical services, Plaintiffs and the Class entered into an implied contract with Defendant in which Defendant agreed to comply with the statutory and common law duties to protect their Private Information and to timely notify them in the event of a data breach.

270. Based on this implicit understanding, Plaintiffs and the Class accepted Defendant's offers and provided Defendant with their Private Information. In exchange for Plaintiffs' and the Class's Private Information, Defendant had an implied duty to safeguard their Private Information through reasonable industry standards.

271. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised.

272. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

273. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice of the Data Breach.

274. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and violated Plaintiffs and the Class Members privacy rights under HIPAA. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the Private Information from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Private Information; and (iii) failing to

disclose to Plaintiffs and the Class at the time they provided their Private Information that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

275. The losses and damages Plaintiffs and Class Members sustained were the direct and proximate result of Defendant's breach of the implied contract with Plaintiffs and Class Members.

COUNT V – BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

276. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

277. Defendant was fully aware of the confidential nature of the Private Information of Plaintiffs and Class Members that it was provided.

278. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class was governed by promises and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

279. Plaintiffs and Class Members provided their respective Private Information to Defendant, with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

280. Plaintiffs and Class Members provided their respective Private Information to Defendant, with the explicit and implicit understandings that Defendant would take precautions to protect their Private Information from unauthorized access, acquisition, appropriation, disclosure,

encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

281. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

282. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiffs and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

283. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages as alleged herein.

284. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

285. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' Private Information. Defendant knew its data systems and protocols for accepting

and securing Plaintiffs and Class Members' Private Information had security and other vulnerabilities that placed Plaintiffs' and Class Members' Private Information in jeopardy.

286. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) 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; (e) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' Private Information in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Plaintiffs' and Class Members' Private Information.

COUNT VI – BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

287. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

288. A relationship existed between Plaintiffs and Class Members and Defendant in which Plaintiffs and the Class put their trust in Defendant to protect their Private Information. Defendant accepted this duty and obligation when it received Plaintiffs' and the Class Members' Private Information.

289. Plaintiffs and the Class Members entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and refrain from disclosing their Private Information to unauthorized third parties.

290. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's Private Information involved an unreasonable risk of harm to Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

291. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and the Class's information in Defendant's possession was adequately secured and protected.

292. Defendant also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiffs' and the Class's Private Information. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Defendant was entrusted with Plaintiffs' and the Class's Private Information.

293. Defendant breached its fiduciary duty that it owed Plaintiffs and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the Private Information of Plaintiffs and the Class Members.

294. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiffs and the Class.

295. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiffs and the Class.

296. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

COUNT VII – UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

297. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

298. Plaintiffs and the Class Members conferred a monetary benefit on Defendant by providing Defendant with profits from Plaintiffs' and Class Members' medical services.

299. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and the Class Members and accepted that monetary benefit.

300. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

301. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

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

303. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

304. Plaintiffs and Class Members have no adequate remedy at law. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) 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; (e) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' Private Information in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Plaintiffs' and Class Members' Private Information.

305. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

306. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that they unjustly received.

COUNT VIII – DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

307. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

308. Under GA Code § 9-4-2, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

309. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Class's Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their v and remains at imminent risk that further compromises of their Private Information will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

310. Plaintiffs and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Class's Private Information, including Social Security numbers, medical records, and financial account information, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete Private Information it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers and financial information.

311. Pursuant to its authority under GA Code § 9-4-2, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure the Private Information of Plaintiffs and the Class;
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information; and
- c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Class harm.

312. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' Private Information. Specifically, this injunction should, among other things, direct Defendant to:

- a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;
- b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;
- c. regularly test its systems for security vulnerabilities, consistent with industry standards;
- d. implement an education and training program for appropriate employees regarding cybersecurity.

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

occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

314. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. 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.

315. 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 Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT IX – Bailment
(On Behalf of Plaintiffs and the Class)

316. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

317. Plaintiffs’ and Class Members’ Private Information was provided to Defendant.

318. In delivering their Private Information, Plaintiffs and Class members intended and understood that their Private Information would be adequately safeguarded and protected.

319. Defendant accepted Plaintiffs’ and Class Members’ Private Information.

320. By accepting possession of Plaintiffs’ and Class Members’ Private Information, Defendant understood that Plaintiffs and the Class expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

321. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their Private Information.

322. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' Private Information.

323. Defendant further breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

324. Defendant failed to return, purge, or delete the Private Information belonging to Plaintiffs and Class Members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

325. As a direct and proximate result of Defendant's breach of its duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

326. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs' and Class Members' Private Information that was entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Ga. Code Ann., § 9-11-23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory 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 and the general public as requested herein, including, but not limited to:

- i. 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;
- ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- iv. 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;
- v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;
- vi. Ordering that Defendant conduct regular database scanning and securing checks; and

- vii. 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.
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
- e. A judgment in favor of Plaintiffs 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.

VIII. DEMAND FOR JURY TRIAL

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

Dated: October 11, 2024

Respectfully submitted,

/s/ Nickolas J. Hagman

Nickolas J. Hagman (Admitted *pro hac vice*)

**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**

135 S. LaSalle, Suite 3210

Chicago, Illinois 60603

Telephone: (312) 782-4880

Facsimile: (312) 782-4485

nhagman@caffertyclobes.com

William B. Federman (Admitted *pro hac vice*)

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

Telephone: (405) 235-1560

wbf@federmanlaw.com

Interim Co-Lead Counsel

Brian P. Adams

Georgia Bar No. 142474

Mary Beth Hand

Georgia Bar No. 322836

ADAMS LAW FIRM

598 D.T. Walton Sr. Way
Macon, GA 31201
Phone: (478) 238-231
brian@brianadamslaw.com
mbhand@brianadamslaw.com

James M. Evangelista
Georgia Bar. No. 707807
EVANGELISTA WORLEY LLC
500 Sugar Mill Road, Suite 245A
Atlanta, Georgia 30350
Phone: (404) 205-8400
Fax: (404) 205-8395
jim@ewlawllc.com

Joseph B. Alonso
Georgia Bar No.: 013627
ALONSO WIRTH
1708 Peachtree Street, NW
Suite 207
Atlanta, GA 30309
Tel: (678)-928-4472
jalonso@alonsowirth.com

Samuel J. Strauss
Raina C. Borrelli
STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

/s/ Michael A. Caplan
Michael A. Caplan
Georgia Bar No. 601039
T. Brandon Waddell
Georgia Bar No. 252639
CAPLAN COBB LLC
75 Fourteenth Street, NE, Suite 2700
Atlanta, Georgia 30309
Tel: (404) 596-5600
Fax: (404) 596-5604
mcaplan@caplancobb.com
bwaddell@caplancobb.com

Additional Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I hereby certify that I have this day caused a true and correct copy of the foregoing to be filed with the Clerk of Court using the Peachcourt system, which will serve a true and correct copy of the same upon all counsel of record, who have consented to electronic service of documents.

This 11th day of October, 2024.

/s/ Michael A. Caplan
Michael A. Caplan
Georgia Bar No. 601039
mcaplan@caplancobb.com

Counsel for Plaintiffs and the Class