

1 Robert S. Green (State Bar No. 136183)
2 James Robert Noblin (State Bar No. 114442)
3 Emrah M. Sumer (State Bar No. 329181)
4 **GREEN & NOBLIN, P.C.**
5 2200 Larkspur Landing Circle, Suite 101
6 Larkspur, California 94939
7 Telephone: (415) 477-6700
8 Facsimile: (415) 477-6710
9 Email: gnecf@classcounsel.com

10 *Counsel for Plaintiff and the Proposed Class*

11 **UNITED STATES DISTRICT COURT**
12 **SOUTHERN DISTRICT OF CALIFORNIA**

13 CHAYA CLARK, individually and
14 on behalf of all others similarly
15 situated and on behalf of the general
16 public,

17 Plaintiff,

18 v.

19 NETGAIN TECHNOLOGY, LLC,
20 and CARESOUTH CAROLINA,
21 INC.

22 Defendants.

Case No.: '21CV1432 DMS BLM

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff, Chaya Clark (“Ms. Clark”), individually and on behalf of all
2 others similarly situated and on behalf of the general public, for her Class Action
3 Complaint, brings this action against Defendants Netgain Technology, LLC
4 (“Netgain”) and CareSouth Carolina, Inc. (“CareSouth”) based on personal
5 knowledge and the investigation of counsel and alleges as follows:

6 **I. INTRODUCTION**

7 1. With this action, Plaintiff seeks to hold Defendants responsible for
8 the harms it caused her and the hundreds of thousands of other similarly situated
9 persons in the massive and preventable ransomware attack that took place on or
10 around December 3, 2020 by which cyber criminals infiltrated Defendants’
11 inadequately protected network servers where highly sensitive personal and
12 medical information was being kept unprotected (“Data Breach” or “Breach”).¹

13 2. The cybercriminals gained access to certain of Defendants’ network
14 servers with the apparent intention of profiting from such access. Defendant
15 Netgain chose to negotiate with the criminals, paying a significant amount of
16 money to them in exchange for a promise from the attackers that they would
17 delete the copies of the data that was in their possession, and that they would not
18 publish, sell or otherwise share the data.

19 3. Defendant Netgain is a cloud hosting and information technology
20 services provider that provides services to several organizations in the healthcare
21 and accounting industries nationwide.²

22
23
24
25 ¹ The Data Breach appears on the U.S. Department of Health and Human
26 Services’ online public breach tool and shows that approximately 76,035
27 CareSouth patients were affected by the Data Breach. *See* U.S. Department of
28 Health & Human Services - Office for Civil Rights (hhs.gov) (last accessed June
10, 2021).

² <https://netgaincloud.com/> (last accessed June 17, 2021).

1 4. On its website, Netgain touts its services as being “secure” and
2 “specialized” and promotes itself as “the industry standard for secure and scalable
3 IT-as-a-Service for healthcare and financial services organizations.”³

4 5. In a recent blog post titled “What we learned as a ransomware victim
5 – so you don’t become one,” which addresses the Data Breach, Netgain describes
6 its experience as “both humbling and galvanizing.”⁴ Netgain also writes that,
7 “[w]hile its true that [managed service providers and technology partners
8 (including us)] can significantly reduce the burden of security on our clients and
9 their teams, *the responsibility is still shared*” (emphasis added).

10 6. Defendant CareSouth, one of Defendant Netgain’s clients with which
11 it shares this burden of data security, is a community health center providing a
12 comprehensive set of services to its patients, “from pediatrics to pharmacy to
13 community outreach.”⁵

14 7. Plaintiff and Class members were required, as patients of CareSouth,
15 to provide Defendants with their “Personal and Medical Information” (defined
16 below), with the assurance that such information would be kept safe from
17 unauthorized access. By taking possession and control of Plaintiff’s and Class
18 members’ Personal and Medical Information, Defendants assumed a duty to
19 securely store and protect the Personal and Medical Information of Plaintiff and
20 the Class.

21 8. Defendants breached this duty and betrayed the trust of Plaintiff and
22 Class members by failing to properly safeguard and protect their Personal and
23 Medical Information, thus enabling cyber criminals to access, acquire,
24
25

26 ³ *Id.*

27 ⁴ See <https://netgaincloud.com/blog/what-we-learned-as-a-ransomware-victim-so-you-dont-become-one/> (last accessed June 17, 2021).

28 ⁵ See <https://www.caresouth-carolina.com/about> (last accessed June 17, 2021).

1 appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse,
2 and/or view it.

3 9. The Personal and Medical Information compromised includes names
4 and addresses, medical record numbers, dates of birth, social security numbers,
5 health insurance policy and identification numbers, insurance claims, explanation
6 of benefits, statements, clinical notes, referral requests, laboratory reports,
7 decision not to vaccinate forms, authorization requests for services, treatment
8 approvals, records requests, immunization information, vaccine records,
9 prescription requests, release of information forms, subpoena records requests,
10 medical record disclosure logs, incident reports, invoices, correspondence with
11 patients, student identification numbers, bank account numbers, employment
12 related documents, court documents, Drug Enforcement Agency certificates,
13 payroll withholding and insurance deduction authorizations, benefit and tax forms,
14 employee health information and some medical records.⁶

15 10. Defendants' misconduct – failing to timely implement adequate and
16 reasonable measures to protect Plaintiff's Personal and Medical Information,
17 failing to timely detect the Data Breach, failing to take adequate steps to prevent
18 and stop the Data Breach, failing to disclose the material facts that they did not
19 have adequate security practices in place to safeguard the Personal and Medical
20 Information, failing to honor their promises and representations to protect
21 Plaintiff's and Class members' Personal and Medical Information, and failing to
22 provide timely and adequate notice of the Data Breach – caused substantial harm
23 and injuries to Plaintiff and Class members across the United States.

24 11. Due to Defendants' negligence and data security failures, cyber
25 criminals obtained and now possess everything they need to commit personal and
26

27 _____
28 ⁶ <https://www.infosecurity-magazine.com/news/woodcreek-netgain-ransomware-attack/> (last accessed June 10, 2021).

1 medical identity theft and wreak havoc on the financial and personal lives of
2 hundreds of thousands of individuals for decades to come.

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

12 13. Plaintiff brings this action individually and on behalf of the Class and
13 seeks actual damages, statutory damages, punitive damages, and restitution, with
14 attorney fees, costs, and expenses, under state consumer protection and unfair and
15 deceptive practices acts, and further sues Defendants for, among other causes of
16 action, negligence (including negligence *per se*). Plaintiff also seeks declaratory
17 and injunctive relief, including significant improvements to Defendants' data
18 security systems and protocols, future annual audits, Defendants-funded long-term
19 credit monitoring services, and other remedies as the Court sees necessary and
20 proper.

21 **II. THE PARTIES**

22 14. Plaintiff Chaya Clark is a citizen and resident of the State of South
23 Carolina.

24 15. Ms. Clark was a patient of, and received medical services from,
25 CareSouth. Her Personal and Medical Information was within the possession and
26 control of Defendants at the time of the Data Breach.

1 16. Plaintiff received a letter from CareSouth dated May 17, 2021,
2 informing her that her Personal and Medical Information was involved in the Data
3 Breach. *See Exhibit 1*, the “Notice.”

4 17. As required in order to obtain medical services from CareSouth,
5 Plaintiff provided CareSouth with highly sensitive personal, financial, health, and
6 insurance information.

7 18. Because of Defendants’ negligence leading up to and including the
8 period of the Data Breach, Plaintiff’s Personal and Medical Information is now in
9 the hands of cyber criminals and Plaintiff is under an imminent and substantially
10 likely risk of identity theft and fraud, including medical identity theft and medical
11 fraud.

12 19. The imminent risk of medical identity theft and fraud that Plaintiff
13 and Class members now face is substantial, certainly impending, and continuous
14 and ongoing because of the negligence of Defendants, which negligence led to the
15 Data Breach. Plaintiff and Class members have already been forced to spend time
16 responding to, and attempting to mitigate the harms of, the Data Breach in an
17 effort to determine how best to protect themselves from certainly impending
18 identity theft and medical information fraud. These efforts are continuous and
19 ongoing and will be for years to come.

20 20. As a direct and proximate result of the Data Breach, Plaintiff and the
21 Class will be required to purchase a yearly subscription to identity theft protection
22 and credit monitoring upon the expiration of the woefully inadequate twelve (12)
23 months of free monitoring provided to them by Defendants. The purchase of
24 identity theft protection and credit monitoring will be necessary in order to protect
25 themselves from medical identity theft and other types of fraud, of which they are
26 now substantially at risk. This subscription will need to be renewed yearly for the
27 rest of their lives.

28

1 21. Plaintiff and Class members have also suffered injury directly and
2 proximately caused by the Data Breach, including damages and diminution in
3 value of their Personal and Medical Information that was entrusted to Defendants
4 for the sole purpose of obtaining medical services necessary for their health and
5 well-being, with the understanding that Defendants would safeguard this
6 information against disclosure. Additionally, Plaintiff’s and Class members’
7 Personal and Medical Information is at continued risk of compromise and
8 unauthorized disclosure as it remains in the possession of Defendants and is
9 subject to further breaches so long as Defendants fail to undertake appropriate and
10 adequate measures to protect it.

11 22. Defendant Netgain is a cloud hosting and information technology
12 services provider that provides services to several organizations in the healthcare
13 and accounting industries nationwide.

14 23. Netgain is headquartered in Minnesota.

15 24. Defendant CareSouth, one of Defendant Netgain’s clients with which
16 it shares this burden of data security, is a community health center providing a
17 comprehensive set of services to its patients, from pediatrics to pharmacy to
18 community outreach.

19 25. CareSouth is headquartered in South Carolina.

20 26. As part of Defendants’ business, Defendants collect substantial
21 amounts of Personal and Medical Information. The information Defendants collect
22 qualifies as “Personal information” under state data breach and information
23 privacy acts. The medical information that Defendants collect qualifies as
24 “Medical Information” under the federal Health Information Portability and
25 Accountability Act (“HIPAA”).

26 **III. JURISDICTION AND VENUE**

27 27. This Court has diversity jurisdiction over this action under the Class
28 Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action

1 involving more than 100 class members, the amount in controversy exceeds
2 \$5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class
3 are citizens of states that differ from Defendants.

4 28. This Court has personal jurisdiction over Defendants because
5 Defendant Netgain conducts much of its business in and has sufficient minimum
6 contacts with California.

7 29. Venue is likewise proper as to Defendants in this District under 28
8 U.S.C. § 1391(a)(1) because Defendant Netgain conducts business through this
9 District (including promoting, selling, marketing, and distributing the Netgain
10 brand and services at issue).

11 **IV. FACTUAL ALLEGATIONS**

12 **A. The California Attorney General Notice**

13 30. On or about December 3, 2020, Defendant Netgain’s network servers
14 were subject to a ransomware attack through which unauthorized third-party
15 cybercriminals gained access to Plaintiff’s and Class members’ Personal and
16 Medical Information.

17 31. CareSouth and multiple other healthcare facilities who contracted
18 with Defendant Netgain as their vendor began filing with various state Attorneys
19 General (including California) sample “Notice of Data Security Incident” letters
20 that mirrored the language of the Notice sent to Plaintiff and Class members.

21 32. Pursuant to California Civ. Code § 1798.82(f), “[a] person or
22 business that is required to issue a security breach notification pursuant to
23 [§ 1798.82(a)] to more than 500 California residents as a result of a single breach
24 of the security system shall electronically submit a single sample copy of that
25 security breach notification, excluding any personally identifiable information, to
26 the Attorney General.”

27 33. Plaintiff’s and Class members’ Personal and Medical Information is
28 “personal information” as defined by California Civ. Code § 1798.82(h).

1 34. Pursuant to California Civ. Code § 1798.82(a)(1), data breach
2 notification letters are sent to residents of California “whose unencrypted
3 personal information was, or is reasonably believed to have been, acquired by an
4 unauthorized person” due to a “breach of the security of the system.”

5 35. California Civ. Code § 1798.82(g) defines “breach of the security of
6 the system” as the “unauthorized acquisition of computerized data that
7 compromises the security, confidentiality, or integrity of personal information
8 maintained by the person or business.”

9 36. The Data Breach was a “breach of the security of the system” as
10 defined by California Civ. Code § 1798.82(g).

11 37. Plaintiff’s and Class members’ unencrypted personal information was
12 acquired by an unauthorized cybercriminal or cybercriminals as a result of the
13 Data Breach.

14 38. Defendants reasonably believe Plaintiff’s and Class members’
15 unencrypted personal information was acquired by an unauthorized person as a
16 result of the Data Breach.

17 39. The security, confidentiality, or integrity of Plaintiff’s and Class
18 members’ unencrypted personal information was compromised as a result of the
19 Data Breach.

20 40. Defendants reasonably believe the security, confidentiality, or
21 integrity of Plaintiff’s and Class members’ unencrypted personal information was
22 compromised as a result of the Data Breach.

23 41. Plaintiff’s and Class members’ unencrypted personal information that
24 was acquired by an unauthorized person as a result of the Data Breach was viewed
25 by unauthorized persons.

26 42. Defendants reasonably believe Plaintiff’s and Class members’
27 unencrypted personal information that was acquired by an unauthorized person as
28 a result of the Data Breach was viewed by unauthorized persons.

1 43. It is reasonable to infer that Plaintiff’s and Class members’
2 unencrypted personal information that was acquired by an unauthorized person as
3 a result of the Data Breach was viewed by unauthorized persons.

4 44. It should be presumed that Plaintiff’s and Class members’
5 unencrypted personal information that was acquired by an unauthorized person as
6 a result of the Data Breach was viewed by unauthorized persons.

7 45. After receiving letters similar to those sent pursuant to California Civ.
8 Code § 1798.82(a)(1) – and filed with the Attorney General of California in
9 accordance with California Civ. Code § 1798.82(f) – it is reasonable for
10 recipients, including Plaintiff and Class members in this case, to (i) believe that
11 the risk of future harm (including identity theft) is real and imminent, and (ii) take
12 steps to mitigate that risk of future harm.

13 **B. The Data Breach and Defendants’ Failed Response**

14 46. It is apparent from the various notices and sample notices of the Data
15 Breach sent to Plaintiff, the Class, and state Attorneys General that the Personal
16 and Medical Information contained within these servers was not encrypted.

17 47. Following discovery of the Data Breach, Defendants began working
18 with cybersecurity experts to investigate and address the Data Breach. Based upon
19 the investigation, the attackers were able to access certain network servers
20 containing the Personal and Medical Information at issue, which was being held,
21 unencrypted and unprotected.

22 48. Upon information and belief, the unauthorized third-party
23 cybercriminals gained access to the Personal and Medical Information with the
24 intent of engaging in misuse of the Personal and Medical Information, including
25 marketing and selling Plaintiff’s and Class members’ Personal and Medical
26 Information on the dark web.

27 49. Despite knowing that hundreds of thousands of patients across the
28 nation were in danger as a result of the Data Breach, Defendants did nothing to

1 warn Plaintiff or Class members until six (6) months after learning of the Data
2 Breach – an unreasonable amount of time under any objective standard.

3 50. Apparently, Defendants chose to complete their investigation and
4 develop a list of talking points before giving Plaintiff and Class members the
5 information they needed to protect themselves against fraud and identity theft.

6 51. In spite of the severity of the Data Breach, Defendants have done
7 very little to protect Plaintiff and the Class. For example, in the Notice,
8 Defendants only provide twelve (12) months of identity theft and credit
9 monitoring protection.

10 52. In effect, Defendants are shirking their responsibility for the harm
11 and increased risk of harm they have caused Plaintiff and members of the Class,
12 including the distress and financial burdens the Data Breach has placed upon the
13 shoulders of the Data Breach victims.

14 53. Defendants also attempt to avoid responsibility for the future harms
15 Plaintiff and the Class now face by including in the Notice a description of
16 Netgain’s response to the Data Breach, including payment of a “significant
17 amount” to the cybercriminals “in exchange for promises that the attacker will
18 delete all copies of the data and that it will not publish, sell, or otherwise share the
19 data.”

20 54. However, this information fails to provide the consolation Plaintiff
21 and Class members seek and certainly falls far short of eliminating the substantial
22 risk of fraud and identity theft Plaintiff and the Class now face.

23 55. Ransomware creators “are criminals without any ethics,” so there is
24 no guarantee they will do what they promise to do in exchange for the ransom
25 money.⁷

26
27
28 ⁷ <https://enterprise.comodo.com/does-paying-ransomware-work.php> (last accessed
June 10, 2021).

1 56. To make matters worse, Defendants’ attackers actually gained access
2 to, and possession of, Plaintiff’s and Class members’ Personal and Medical
3 Information. While many ransomware attacks merely involve the attacker gaining
4 control of the computer or network without access to the victims’ information, the
5 ransomware attack on Defendants’ systems gave the attackers access to and
6 possession of Plaintiff’s and Class members’ Personal and Medical Information.

7 57. Moreover, paying the ransom as Netgain did will only encourage
8 attackers to carry out these types of cyberattacks on Netgain’s system networks in
9 the future.

10 58. Defendants failed to adequately safeguard Plaintiff’s and Class
11 members’ Personal and Medical Information, allowing cyber criminals to access
12 this wealth of priceless information for nearly six months before warning the
13 criminals’ victims to be on the lookout, and now offer them almost no remedy or
14 relief.

15 59. Defendants failed to spend sufficient resources on cybersecurity
16 training and adequate data security measures and protocols.

17 60. Defendants had obligations created by HIPAA, reasonable industry
18 standards, common law, state statutory law, and their own assurances and
19 representations to keep patients’ Personal and Medical Information confidential
20 and to protect such Personal and Medical Information from unauthorized access.

21 61. Plaintiff and Class members were required to provide their Personal
22 and Medical Information to Defendants with the reasonable expectation and
23 mutual understanding that Defendants would comply with their obligations to
24 keep such information confidential and secure from unauthorized access.

25 62. The stolen Personal and Medical Information at issue has great value
26 to the ransomware attackers, due to the large number of individuals affected and
27 the fact that health insurance information, bank account information, and Social
28 Security numbers were part of the data that was compromised.

1 **C. Defendants had an Obligation to Protect Personal and Medical**
2 **Information under Federal Law and the Applicable Standard**
3 **of Care**

4 63. Defendants are covered by HIPAA (45 C.F.R. § 160.102). As such,
5 they are required to comply with the HIPAA Privacy Rule and Security Rule, 45
6 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of
7 Individually Identifiable Health Information”), and Security Rule (“Security
8 Standards for the Protection of Electronic Protected Health Information”), 45
9 C.F.R. Part 160 and Part 164, Subparts A and C.

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

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

17 66. HIPAA requires Defendants to “comply with the applicable
18 standards, implementation specifications, and requirements” of HIPAA “with
19 respect to electronic protected health information.” 45 C.F.R. § 164.302.

20 67. “Electronic protected health information” is “individually identifiable
21 health information ... that is (i) transmitted by electronic media; maintained in
22 electronic media.” 45 C.F.R. § 160.103.

23 68. HIPAA’s Security Rule requires Defendants to do the following:

- 24 a. Ensure the confidentiality, integrity, and availability of all
25 electronic protected health information the covered entity or
26 business associate creates, receives, maintains, or transmits;
- 27 b. Protect against any reasonably anticipated threats or hazards to
28 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.

69. HIPAA also requires Defendants 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).

70. HIPAA also requires Defendants 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).

71. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants 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.*”⁸

72. Defendants were also prohibited by the Federal Trade Commission Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. As described before, Defendants are required to protect Plaintiff’s and Class members’ Personal and Medical Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

⁸ Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

1 74. In addition to their obligations under federal and state laws,
2 Defendants owed a duty to Plaintiff and Class members to exercise reasonable
3 care in obtaining, retaining, securing, safeguarding, deleting, and protecting the
4 Personal and Medical Information in their possession from being compromised,
5 lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a
6 duty to Plaintiff and Class members to provide reasonable security, including
7 consistency with industry standards and requirements, and to ensure that their
8 computer systems, networks, and protocols adequately protected the Personal and
9 Medical Information of the Class.

10 75. Defendants owed a duty to Plaintiff and the Class to design, maintain,
11 and test their computer systems and networks to ensure that the Personal and
12 Medical Information in Defendants' possession was adequately secured and
13 protected.

14 76. Defendants owed a duty to Plaintiff and the Class to create and
15 implement reasonable data security practices and procedures to protect the
16 Personal and Medical Information in their possession.

17 77. Defendants owed a duty to Plaintiff and the Class to implement
18 processes that would detect a breach on their data security systems in a timely
19 manner.

20 78. Defendants owed a duty to Plaintiff and the Class to act upon data
21 security warnings and alerts in a timely fashion.

22 79. Defendants owed a duty to Plaintiff and the Class to disclose if their
23 computer systems and data security practices were inadequate to safeguard
24 individuals' Personal and Medical Information from theft because such an
25 inadequacy would be a material fact in the decision to entrust Personal and
26 Medical Information with Defendants.

27 80. Defendants owed a duty to Plaintiff and the Class to disclose in a
28 timely and accurate manner when data breaches occurred.

1 81. Defendants owed a duty of care to Plaintiff and the Class because
2 they were foreseeable and probable victims of any inadequate data security
3 practices.

4 **D. Defendants were on Notice of Cyber Attack Threats in the**
5 **Healthcare Industry and of the Inadequacy of their Data**
6 **Security**

7 82. Defendants were on notice that companies in the healthcare industry
8 were targets for cyberattacks.

9 83. Defendants were on notice that the FBI has recently been concerned
10 about data security in the healthcare industry. In August 2014, after a cyberattack
11 on Community Health Systems, Inc., the FBI warned companies within the
12 healthcare industry that hackers were targeting them. The warning stated that
13 “[t]he FBI has observed malicious actors targeting healthcare related systems,
14 perhaps for the purpose of obtaining the Protected Healthcare Information (PHI)
15 and/or Personally Identifiable Information (PII).”⁹

16 84. The American Medical Association (“AMA”) has also warned
17 healthcare companies about the importance of protecting their patients’
18 confidential information:

19 Cybersecurity is not just a technical issue; it’s a patient safety
20 issue. AMA research has revealed that 83% of physicians
21 work in a practice that has experienced some kind of
22 cyberattack. Unfortunately, practices are learning that
23 cyberattacks not only threaten the privacy and security of
24 patients’ health and financial information, but also patient
25 access to care.¹⁰

26 ⁹ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*,
27 REUTERS (Aug. 2014), <http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>.

28 ¹⁰ 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>.

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

5 86. Defendants were on notice that the federal government has been
6 concerned about healthcare company data encryption. Defendants knew they kept
7 protected health information in on their servers and yet it appears Defendants did
8 not encrypt this information.

9 87. The United States Department of Health and Human Services' Office
10 for Civil Rights urges the use of encryption of data containing sensitive personal
11 information. As long ago as 2014, the Department fined two healthcare companies
12 approximately two million dollars for failing to encrypt laptops containing
13 sensitive personal information. In announcing the fines, Susan McAndrew, the
14 DHHS's Office of Human Rights' deputy director of health information privacy,
15 stated "[o]ur message to these organizations is simple: encryption is your best
16 defense against these incidents."¹¹

17 88. As covered entities or business associates under HIPAA, Defendants
18 should have known their systems were prone to ransomware and other types of
19 cyberattacks and sought better protection for the Personal and Medical
20 Information accumulating in their system networks.

21 **E. Cyber Criminals Will Use Plaintiff's and Class Members'**
22 **Personal and Medical Information to Defraud Them**

23 89. Plaintiff and Class members' Personal and Medical Information is of
24 great value to hackers and cyber criminals, and the data stolen in the Data Breach
25

26
27 ¹¹“Stolen Laptops Lead to Important HIPAA Settlements,” U.S. Dep't of Health
28 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>.

1 will be used in a variety of sordid ways for criminals to exploit Plaintiff and the
2 Class members and to profit off their misfortune.

3 90. Each year, identity theft causes tens of billions of dollars of losses to
4 victims in the United States.¹² For example, with the Personal and Medical
5 Information stolen in the Data Breach, including Social Security numbers, identity
6 thieves can open financial accounts, apply for credit, file fraudulent tax returns,
7 commit crimes, create false driver's licenses and other forms of identification and
8 sell them to other criminals or undocumented immigrants, steal government
9 benefits, give breach victims' names to police during arrests, and many other
10 harmful forms of identity theft.¹³ These criminal activities have and will result in
11 devastating financial and personal losses to Plaintiff and Class members.

12 91. Personal and Medical Information is such a valuable commodity to
13 identity thieves that once it has been compromised, criminals will use it and trade
14 the information on the cyber black-market for years.¹⁴

15 92. For example, it is believed that certain Personal and Medical
16 Information compromised in the 2017 Experian data breach was being used, three
17 years later, by identity thieves to apply for COVID-19-related benefits in the state
18 of Oklahoma.¹⁵

19
20
21 ¹²“Facts + Statistics: Identity Theft and Cybercrime,” Insurance Info. Inst.,
22 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
(discussing Javelin Strategy & Research's report “2018 Identity Fraud: Fraud
Enters a New Era of Complexity”).

23 ¹³See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social*
24 *Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

25 ¹⁴ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is*
26 *Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007,
27 <https://www.gao.gov/assets/270/262904.html>

28 ¹⁵ See <https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html>; see also <https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>.

1 93. This was a financially motivated Data Breach, as apparent from the
2 ransom money sought and gained by the cyber criminals, who will continue to
3 seek to profit off of the sale of Plaintiff's and the Class members' Personal and
4 Medical Information on the dark web. The Personal and Medical Information
5 exposed in this Data Breach is valuable to identity thieves for use in the kinds of
6 criminal activity described herein.

7 94. These risks are both certainly impending and substantial. As the FTC
8 has reported, if hackers get access to personally identifiable information, they will
9 use it.¹⁶

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

13 [I]n some cases, stolen data may be held for up to a year or more
14 before being used to commit identity theft. Further, once stolen
15 data have been sold or posted on the Web, fraudulent use of that
16 information may continue for years. As a result, studies that
17 attempt to measure the harm resulting from data breaches cannot
necessarily rule out all future harm.¹⁷

18 96. For instance, with a stolen Social Security number, which is part of
19 the Personal and Medical Information compromised in the Data Breach, someone
20 can open financial accounts, get medical care, file fraudulent tax returns, commit
21 crimes, and steal benefits.¹⁸ Identity thieves can also use the information stolen
22 from Plaintiff and Class members to qualify for expensive medical care and leave
23 them and their contracted health insurers on the hook for massive medical bills.

24 ¹⁶Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N
25 (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

26 ¹⁷*Data Breaches Are Frequent*, *supra* note 11.

27 ¹⁸ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social*
28 *Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

1 97. Medical identity theft is one of the most common, most expensive,
2 and most difficult-to-prevent forms of identity theft. According to Kaiser Health
3 News, “medical-related identity theft accounted for 43 percent of all identity thefts
4 reported in the United States in 2013,” which is more than identity thefts involving
5 banking and finance, the government and the military, or education.¹⁹

6 98. “Medical identity theft is a growing and dangerous crime that leaves
7 its victims with little to no recourse for recovery,” reported Pam Dixon, executive
8 director of World Privacy Forum. “Victims often experience financial
9 repercussions and worse yet, they frequently discover erroneous information has
10 been added to their personal medical files due to the thief’s activities.”²⁰

11 99. As indicated by James Trainor, second in command at the FBI’s
12 cyber security division: “Medical records are a gold mine for criminals—they can
13 access a patient’s name, DOB, Social Security and insurance numbers, and even
14 financial information all in one place. Credit cards can be, say, five dollars or
15 more where [personal health information] can go from \$20 say up to—we’ve seen
16 \$60 or \$70 [(referring to prices on dark web marketplaces)].”²¹ A complete
17 identity theft kit that includes health insurance credentials may be worth up to
18 \$1,000 on the black market.²²

19 100. If cyber criminals manage to access financial information, health
20 insurance information, and other personally sensitive data—as they did here—
21

22 ¹⁹ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser
23 Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

24 ²⁰ *Id.*

25 ²¹ IDExperts, *You Got It, They Want It: Criminals Targeting Your Private*
26 *Healthcare Data, New Ponemon Study Shows*,
<https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>.

27 ²² *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS:
28 Key findings from The Global State of Information Security Survey 2015,
<https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.

1 there is no limit to the amount of fraud to which Defendants may expose the
2 Plaintiff and Class members.

3 101. A study by Experian found that the average total cost of medical
4 identity theft is “about \$20,000” per incident, and that a majority of victims of
5 medical identity theft were forced to pay out-of-pocket costs for healthcare they
6 did not receive in order to restore coverage.²³ Almost half of medical identity
7 theft victims lose their healthcare coverage as a result of the incident, while nearly
8 one-third saw their insurance premiums rise, and forty percent were never able to
9 resolve their identity theft at all.²⁴

10 102. As described above, identity theft victims must spend countless hours
11 and large amounts of money repairing the impact to their credit.²⁵

12 103. Defendants’ failure to offer sufficient identity monitoring to the
13 Class, including to Plaintiff, is egregious. Moreover, Defendants’ offer of one year
14 of identity theft monitoring is woefully inadequate, as the worst is yet to come.

15 104. Victims of the Data Breach, like Plaintiff and other Class members,
16 must spend many hours and large amounts of money protecting themselves from
17 the future negative impacts to their credit because of the Data Breach.²⁶

20 ²³ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET
21 (Mar, 3, 2010), [https://www.cnet.com/news/study-medical-identity-theft-is-costly-
22 for-victims/](https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/).

23 ²⁴ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to*
24 *Do After One*, EXPERIAN, [https://www.experian.com/blogs/ask-
25 experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-
26 one/](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/).

27 ²⁵ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4
28 (Sept. 2013), [http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-
theft-victims.pdf](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf).

²⁶ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4
(Sept. 2013), [http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-
theft-victims.pdf](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf).

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

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

- 13 a. Trespass and damage their personal property, including
14 Personal and Medical Information;
- 15 b. Improper disclosure of their Personal and Medical Information;
- 16 c. The imminent and certainly impending injury flowing from
17 potential fraud and identity theft posed by their Personal and
18 Medical Information being placed in the hands of criminals;
- 19 d. The imminent and certainly impending risk of having their
20 confidential medical information used against them by spam
21 callers to defraud them;
- 22 e. Damages flowing from Defendants’ untimely and inadequate
23 notification of the data breach;
- 24 f. Loss of privacy suffered as a result of the Data Breach;
- 25 g. Ascertainable losses in the form of the value of their time
26 reasonably expended to remedy or mitigate the effects of the
27 Data Breach;
- 28

- 1 h. Ascertainable losses in the form of deprivation of the value of
2 patients’ personal information, for which there is a well-
3 established and quantifiable national and international market;
4 and
5 i. The loss of use of and access to their credit, accounts, and/or
6 funds.

7 107. Moreover, Plaintiff and Class members have an interest in ensuring
8 that their information, which remains in the possession of Defendants, is protected
9 from further breaches by the implementation of industry standard and statutorily
10 compliant security measures and safeguards. Defendants have shown themselves
11 to be wholly incapable of protecting Plaintiff’s and Class members’ Personal and
12 Medical Information.

13 108. Plaintiff and Class members are desperately trying to mitigate the
14 damage that Defendants have caused them but, given the kind of Personal and
15 Medical Information Defendants made accessible to hackers, they are certain to
16 incur additional damages. Because identity thieves have their Personal and
17 Medical Information, Plaintiff and all Class members will need to have identity
18 theft monitoring protection for the rest of their lives. Some may even need to go
19 through the long and arduous process of getting a new Social Security number,
20 with all the loss of credit and employment difficulties that come with this
21 change.²⁷

22 109. None of this should have happened. The Data Breach was
23 preventable.

24
25
26
27 ²⁷ *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov.
28 16, 2015), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

1 **F. Defendants Could Have Prevented the Data Breach but Failed**
2 **to Adequately Protect Plaintiff’s and Class Members’ Personal**
3 **and Medical Information**

4 110. Data breaches are preventable.²⁸ As Lucy Thompson wrote in the
5 DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data
6 breaches that occurred could have been prevented by proper planning and the
7 correct design and implementation of appropriate security solutions.”²⁹ She added
8 that “[o]rganizations that collect, use, store, and share sensitive personal data must
9 accept responsibility for protecting the information and ensuring that it is not
10 compromised”³⁰

11 111. “Most of the reported data breaches are a result of lax security and
12 the failure to create or enforce appropriate security policies, rules, and procedures
13 Appropriate information security controls, including encryption, must be
14 implemented and enforced in a rigorous and disciplined manner so that a *data*
15 *breach never occurs.*”³¹

16 112. Defendants required Plaintiff and Class members to surrender their
17 Personal and Medical Information – including but not limited to their names,
18 addresses, Social Security numbers, medical information, and health insurance
19 information – and were entrusted with properly holding, safeguarding, and
20 protecting against unlawful disclosure of such Personal and Medical Information.

21 113. Many failures laid the groundwork for the success (“success” from
22 the cybercriminals’ viewpoint) of the Data Breach, starting with Defendants’
23 failure to incur the costs necessary to implement adequate and reasonable cyber
24

25 ²⁸ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are
26 Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson,
27 ed., 2012)

28 ²⁹ *Id.* at 17.

³⁰ *Id.* at 28.

³¹ *Id.*

1 security protections, procedures and protocols necessary to safeguard Plaintiff's
2 and Class members' Personal and Medical Information.

3 114. Defendants maintained the Personal and Medical Information in a
4 reckless manner on network servers that were left vulnerable to cyberattacks.

5 115. Defendants knew, as a cloud hosting and information technology
6 services provider, of the importance of safeguarding Personal and Medical
7 Information and of the foreseeable consequences that would occur if Plaintiff's
8 and Class members' Personal and Medical Information was stolen, including the
9 significant costs that would be placed on Plaintiff and Class members as a result of
10 a breach of this magnitude.

11 116. The mechanism of the cyberattack and potential for improper
12 disclosure of Plaintiff's and Class members' Personal and Medical Information
13 was a known risk to Defendants, and thus Defendants were on notice that failing
14 to take necessary steps to secure Plaintiff's and Class members' Personal and
15 Medical Information from those risks left that information in a dangerous
16 condition.

17 117. Defendants disregarded the rights of Plaintiff and Class members by,
18 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take
19 adequate and reasonable measures to ensure that their network servers were
20 protected against unauthorized intrusions; (ii) failing to disclose that they did not
21 have adequately robust security protocols and training practices in place to
22 adequately safeguard Plaintiff's and Class members' Personal and Medical
23 Information; (iii) failing to take standard and reasonably available steps to prevent
24 the Data Breach; (iv) concealing the existence and extent of the Data Breach for
25 an unreasonable duration of time; and (v) failing to provide Plaintiff and Class
26 members prompt and accurate notice of the Data Breach.

1 **V. CLASS ACTION ALLEGATIONS**

2 118. Plaintiff incorporates by reference all allegations of the preceding
3 paragraphs as though fully set forth herein.

4 119. Plaintiff brings all claims as class claims under Federal Rule of Civil
5 Procedure 23. Plaintiff asserts all claims on behalf of the proposed Nationwide
6 Class and Subclass, defined as follows:

7 **All persons residing in the United States whose personal and**
8 **medical information was compromised as a result of the**
9 **Data Breach that occurred in December 2020.**

10 **CareSouth Subclass: All patients of CareSouth whose**
11 **personal and medical information was compromised as a**
12 **result of the Data Breach that occurred in December 2020.**

13 120. Also, in the alternative, Plaintiff requests additional Subclass as
14 necessary based on the types of Personal and Medical Information that were
15 compromised.

16 121. Excluded from the Nationwide Class and Subclass are Defendants,
17 any entity in which Defendants have a controlling interest, and Defendants'
18 officers, directors, legal representatives, successors, subsidiaries, and assigns. Also
19 excluded from the Class is any judge, justice, or judicial officer presiding over this
20 matter and members of their immediate families and judicial staff.

21 122. Plaintiff reserves the right to amend the above definitions or to
22 propose alternative or additional Subclass in subsequent pleadings and motions for
23 class certification.

24 123. The proposed Nationwide Class and the Subclass (collectively
25 referred to herein as the "Class" unless otherwise specified) meet the requirements
26 of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).
27
28

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

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

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

16 127. **Superiority:** A class action is superior to other available means of
17 fair and efficient adjudication of the claims of Plaintiff and the Class. The injury
18 suffered by each individual Class member is relatively small in comparison to the
19 burden and expense of individual prosecution of complex and expensive litigation.
20 It would be very difficult, if not impossible, for members of the Class individually
21 to effectively redress Defendants' wrongdoing. Even if Class members could
22 afford such individual litigation, the court system could not. Individualized
23 litigation presents a potential for inconsistent or contradictory judgments.
24 Individualized litigation increases the delay and expense to all parties, and to the
25 court system, presented by the complex legal and factual issues of the case. By
26 contrast, the class action device presents far fewer management difficulties and
27 provides benefits of single adjudication, economy of scale, and comprehensive
28 supervision by a single court.

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

- 5 a. Whether Defendants engaged in the wrongful conduct alleged
6 herein;
- 7 b. Whether Defendants failed to adequately safeguard Plaintiff's
8 and Class members' Personal and Medical Information;
- 9 c. Whether Defendants' systems, networks, and data security
10 practices used to protect Plaintiff's and Class members'
11 Personal and Medical Information violated the FTC Act,
12 HIPAA, and/or state laws and/or Defendants' other duties
13 discussed herein;
- 14 d. Whether Defendants owed a duty to Plaintiff and the Class to
15 adequately protect their Personal and Medical Information, and
16 whether they breached this duty;
- 17 e. Whether Defendants knew or should have known that their
18 computer and network security systems were vulnerable to a
19 data breach;
- 20 f. Whether Defendants' conduct, including their failure to act,
21 resulted in or was the proximate cause of the Data Breach;
- 22 g. Whether Defendants breached contractual duties to Plaintiff and
23 the Class to use reasonable care in protecting their Personal and
24 Medical Information;
- 25 h. Whether Defendants failed to adequately respond to the Data
26 Breach, including failing to investigate it diligently and notify
27 affected individuals in the most expedient time possible and
28

1 without unreasonable delay, and whether this caused damages
2 to Plaintiff and the Class;

3 i. Whether Defendants continue to breach duties to Plaintiff and
4 the Class;

5 j. Whether Plaintiff and the Class suffered injury as a proximate
6 result of Defendants' negligent actions or failures to act;

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

9 l. Whether injunctive relief is appropriate and, if so, what
10 injunctive relief is necessary to redress the imminent and
11 currently ongoing harm faced by Plaintiff and members of the
12 Class and the general public;

13 m. Whether Defendants' actions alleged herein constitute gross
14 negligence; and

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

17 **VI. CAUSES OF ACTION**

18 **A. COUNT I – NEGLIGENCE**

19 129. Plaintiff incorporates by reference all allegations of the preceding
20 paragraphs as though fully set forth herein.

21 130. Defendants solicited, gathered, and stored the Personal and Medical
22 Information of Plaintiff and the Class as part of the operation of their business.

23 131. Upon accepting and storing the Personal and Medical Information of
24 Plaintiff and Class members, Defendants undertook and owed a duty to Plaintiff
25 and Class members to exercise reasonable care to secure and safeguard that
26 information and to use secure methods to do so.

27 132. Defendants had full knowledge of the sensitivity of the Personal and
28 Medical Information, the types of harm that Plaintiff and Class members could

1 and would suffer if the Personal and Medical Information was wrongfully
2 disclosed, and the importance of adequate security.

3 133. Plaintiff and Class members were the foreseeable victims of any
4 inadequate safety and security practices. Plaintiff and the Class members had no
5 ability to protect their Personal and Medical Information that was in Defendants'
6 possession. As such, a special relationship existed between Defendants and
7 Plaintiff and the Class.

8 134. Defendants were well aware of the fact that cyber criminals routinely
9 target large corporations through cyberattacks in an attempt to steal sensitive
10 personal and medical information.

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

17 136. Defendants' duty extended to protecting Plaintiff and the Class from
18 the risk of foreseeable criminal conduct of third parties, which has been
19 recognized in situations where the actor's own conduct or misconduct exposes
20 another to the risk or defeats protections put in place to guard against the risk, or
21 where the parties are in a special relationship. *See* Restatement (Second) of Torts
22 § 302B. Numerous courts and legislatures also have recognized the existence of a
23 specific duty to reasonably safeguard personal information.

24 137. Defendants had duties to protect and safeguard the Personal and
25 Medical Information of Plaintiff and the Class from being vulnerable to
26 cyberattacks by taking common-sense precautions when dealing with sensitive
27 Personal and Medical Information. Additional duties that Defendants owed
28 Plaintiff and the Class include:

- 1 a. To exercise reasonable care in designing, implementing,
2 maintaining, monitoring, and testing Defendants' networks,
3 systems, protocols, policies, procedures and practices to ensure
4 that Plaintiff's and Class members' Personal and Medical
5 Information was adequately secured from impermissible
6 access, viewing, release, disclosure, and publication;
- 7 b. To protect Plaintiff's and Class members' Personal and
8 Medical Information in their possession by using reasonable
9 and adequate security procedures and systems;
- 10 c. To implement processes to quickly detect a data breach,
11 security incident, or intrusion involving their networks and
12 servers; and
- 13 d. To promptly notify Plaintiff and Class members of any data
14 breach, security incident, or intrusion that affected or may have
15 affected their Personal and Medical Information.

16 138. Only Defendants were in a position to ensure that their systems and
17 protocols were sufficient to protect the Personal and Medical Information that
18 Plaintiff and the Class had entrusted to them.

19 139. Defendants breached their duties of care by failing to adequately
20 protect Plaintiff's and Class members' Personal and Medical Information.

21 Defendants breached their duties by, among other things:

- 22 a. Failing to exercise reasonable care in obtaining, retaining
23 securing, safeguarding, deleting, and protecting the Personal
24 and Medical Information in their possession;
- 25 b. Failing to protect the Personal and Medical Information in their
26 possession using reasonable and adequate security procedures
27 and systems;

- 1 c. Failing to adequately and properly audit, test, and train their
- 2 employees regarding how to properly and securely transmit
- 3 and store Personal and Medical Information;
- 4 d. Failing to adequately train their employees to not store
- 5 Personal and Medical Information longer than absolutely
- 6 necessary;
- 7 e. Failing to consistently enforce security policies aimed at
- 8 protecting Plaintiff's and the Class's Personal and Medical
- 9 Information;
- 10 f. Failing to implement processes to quickly detect data breaches,
- 11 security incidents, or intrusions;
- 12 g. Failing to promptly notify Plaintiff and Class members of the
- 13 Data Breach that affected their Personal and Medical
- 14 Information.

15 140. Defendants' willful failure to abide by these duties was wrongful,
16 reckless, and grossly negligent in light of the foreseeable risks and known threats.

17 141. As a proximate and foreseeable result of Defendants' grossly
18 negligent conduct, Plaintiff and the Class have suffered damages and are at
19 imminent risk of additional harms and damages (as alleged above).

20 142. Through Defendants' acts and omissions described herein, including
21 but not limited to Defendants' failure to protect the Personal and Medical
22 Information of Plaintiff and Class members from being stolen and misused,
23 Defendants unlawfully breached their duty to use reasonable care to adequately
24 protect and secure the Personal and Medical Information of Plaintiff and Class
25 members while it was within Defendants' possession and control.

26 143. Further, through their failure to provide timely and clear notification
27 of the Data Breach to Plaintiff and Class members, Defendants prevented Plaintiff
28

1 and Class members from taking meaningful, proactive steps to securing their
2 Personal and Medical Information and mitigating damages.

3 144. As a result of the Data Breach, Plaintiff and Class members have
4 spent time, effort, and money to mitigate the actual and potential impact of the
5 Data Breach on their lives, including but not limited to, closely reviewing and
6 monitoring bank accounts, credit reports, and statements sent from providers and
7 their insurance companies and the eventual payment for credit monitoring and
8 identity theft prevention services following the expiration of the twelve months of
9 free monitoring provided by Defendants.

10 145. Defendants' wrongful actions, inactions, and omissions constituted
11 (and continue to constitute) common law negligence.

12 146. The damages Plaintiff and the Class have suffered (as alleged above)
13 and will suffer were and are the direct and proximate result of Defendants' grossly
14 negligent conduct.

15 147. In addition to its duties under common law, Defendants had
16 additional duties imposed by statute and regulations, including the duties under
17 HIPAA and the FTC Act. The harms which occurred as a result of Defendants'
18 failure to observe these duties, including the loss of privacy, significant risk of
19 identity theft, and Plaintiff's overpayment for goods and services, are the types of
20 harm that these statutes and their regulations were intended to prevent.

21 148. Defendants violated these statutes when they engaged in the actions
22 and omissions alleged herein and Plaintiff's injuries were a direct and proximate
23 result of Defendants' violations of these statutes. Plaintiff therefore is entitled to
24 the evidentiary presumptions for negligence *per se* under Cal. Evid. Code § 669.

25 149. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendants owed a duty
26 to Plaintiff and the Class to provide fair and adequate computer systems and data
27 security to safeguard the Personal and Medical Information of Plaintiff and the
28 Class.

1 150. Defendants are entities covered by HIPAA, 45 C.F.R. §160.102, and
2 as such are required to comply with HIPAA’s Privacy Rule and Security Rule.
3 HIPAA requires Defendants to “reasonably protect” confidential data from “any
4 intentional or unintentional use or disclosure” and to “have in place appropriate
5 administrative, technical, and physical safeguards to protect the privacy of
6 protected health information.” 45 C.F.R. § 164.530(c)(1). HIPAA also requires
7 Defendants to obtain satisfactory assurances that their business associates would
8 appropriately safeguard the protected health information they receive or create on
9 behalf of the Defendants. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and
10 (e). The confidential data at issue in this case constitutes “protected health
11 information” within the meaning of HIPAA.

12 151. HIPAA further requires Defendants to disclose the unauthorized
13 access and theft of the protected health information of Plaintiff and the Class
14 “without unreasonable delay” so that Plaintiff and Class members could take
15 appropriate measures to mitigate damages, protect against adverse consequences,
16 and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404,
17 164.406, and 164.410.

18 152. The FTC Act prohibits “unfair practices in or affecting commerce,”
19 including, as interpreted and enforced by the FTC, the unfair act or practice by
20 businesses, such as Defendants, of failing to use reasonable measures to protect
21 Personal and Medical Information. The FTC publications and orders described
22 above also formed part of the basis of Defendants’ duty in this regard.

23 153. Defendants gathered and stored the Personal and Medical
24 Information of Plaintiff and the Class as part of their business of soliciting their
25 services to their patients, which solicitations and services affect commerce.

26 154. Defendants violated the FTC Act by failing to use reasonable
27 measures to protect the Personal and Medical Information of Plaintiff and the
28

1 Class and by not complying with applicable industry standards, as described
2 herein.

3 155. Defendants breached their duties to Plaintiff and the Class under the
4 FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer
5 systems and/or data security practices to safeguard Plaintiff's and Class members'
6 Personal and Medical Information, and by failing to provide prompt notice
7 without reasonable delay.

8 156. Defendants' failure to comply with applicable laws and regulations
9 constitutes negligence *per se*.

10 157. Plaintiff and the Class are within the class of persons that HIPAA and
11 the FTC Act were intended to protect.

12 158. The harm that occurred as a result of the Data Breach is the type of
13 harm the FTC Act and HIPAA were intended to guard against.

14 159. Defendants breached their duties to Plaintiff and the Class under
15 these laws by failing to provide fair, reasonable, or adequate computer systems
16 and data security practices to safeguard Plaintiff's and the Class's Personal and
17 Medical Information.

18 160. Additionally, Defendants had a duty to promptly notify victims of the
19 Data Breach. For instance, HIPAA required Defendants to notify victims of the
20 Breach within sixty (60) days of the discovery of the Data Breach. Defendants did
21 not notify Plaintiff or Class members of the Data Breach until around December
22 16, 2020.

23 161. Defendants knew on or before June 17, 2020, that unauthorized
24 persons had accessed and/or viewed or were reasonably likely to have accessed
25 and/or viewed private, protected, personal information of Plaintiff and the Class.

26 162. Defendants breached their duties to Plaintiff and the Class by
27 unreasonably delaying and failing to provide notice expeditiously and/or as soon
28 as practicable to Plaintiff and the Class of the Data Breach.

1 163. Defendants’ violation of the FTC Act and HIPAA constitutes
2 negligence *per se*.

3 164. As a direct and proximate result of Defendants’ negligence *per se*,
4 Plaintiff and the Class have suffered, and continue to suffer, damages arising from
5 the Data Breach, as alleged above.

6 165. The injury and harm that Plaintiff and Class members suffered (as
7 alleged above) was the direct and proximate result of Defendants’ negligence *per*
8 *se*.

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

11 **B. COUNT II – INVASION OF PRIVACY**

12 167. Plaintiff incorporates by reference all allegations of the preceding
13 paragraphs as though fully set forth herein.

14 168. California established the right to privacy in Article 1, Section 1 of
15 the California Constitution.

16 169. The State of California recognizes the tort of Intrusion into Private
17 Affairs and adopts the formulation of that tort found in the Restatement (Second)
18 of Torts, which states, “One who intentionally intrudes, physically or otherwise,
19 upon the solitude or seclusion of another or his private affairs or concerns is
20 subject to liability to the other for invasion of his privacy if the intrusion would be
21 highly offensive to a reasonable person.” Restatement (Second) of Torts, § 652B
22 (1977).

23 170. South Carolina also recognizes the tort of Invasion of Privacy.

24 171. Plaintiff and Class members had a legitimate and reasonable
25 expectation of privacy with respect to their Personal and Medical Information and
26 were accordingly entitled to the protection of this information against disclosure to
27 and acquisition by unauthorized third parties.
28

1 172. Defendants owed a duty to its patients, including Plaintiff and Class
2 members, to keep their Personal and Medical Information confidential.

3 173. The unauthorized access, acquisition, appropriation, disclosure,
4 encumbrance, exfiltration, release, theft, use, and/or viewing of Personal and
5 Medical Information, especially the type that is the subject of this action, is highly
6 offensive to a reasonable person.

7 174. The intrusion was into a place or thing that was private and is entitled
8 to be private. Plaintiff and Class members disclosed their Personal and Medical
9 Information to Defendants as part of their receiving medical care and treatment
10 from Defendants, but privately, with the intention that such highly sensitive
11 information would be kept confidential and protected from unauthorized access,
12 acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft,
13 use, and/or viewing. Plaintiff and Class members were reasonable in their belief
14 that such information would be kept private and would not be disclosed without
15 their authorization.

16 175. The Data Breach constitutes an intentional interference with
17 Plaintiff's and Class members' interest in solitude or seclusion, either as to their
18 persons or as to their private affairs or concerns, of a kind that would be highly
19 offensive to a reasonable person.

20 176. Defendants acted with a knowing state of mind when they permitted
21 the Data Breach because they knew their information security practices were
22 inadequate.

23 177. Acting with knowledge, Defendants had notice and knew that their
24 inadequate cybersecurity practices would cause injury to Plaintiff and Class
25 members.

26 178. As a proximate result of Defendants' acts and omissions, Plaintiff's
27 and Class members' Personal and Medical Information was accessed by, acquired
28 by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to,

1 stolen by, used by, and/ or reviewed by third parties without authorization, causing
2 Plaintiff and Class members to suffer damages.

3 179. Unless and until enjoined and restrained by order of this Court,
4 Defendants' wrongful conduct will continue to cause great and irreparable injury
5 to Plaintiff and Class members in that the Personal and Medical Information
6 maintained by Defendants can and will likely again be accessed by, acquired by,
7 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
8 by, used by, and/ or viewed by unauthorized persons.

9 180. Plaintiff and the Class have no adequate remedy at law for the
10 injuries in that a judgment for monetary damages will not end the invasion of
11 privacy for Plaintiff and Class members.

12 **C. COUNT III – BREACH OF THIRD-PARTY BENEFICIARY**
13 **CONTRACT**

14 181. Plaintiff incorporates by reference all allegations of the preceding
15 paragraphs as though fully set forth herein.

16 182. Plaintiff brings this claim for breach of third-party beneficiary
17 contract against Defendants on behalf of the Class.

18 183. Defendants entered into contracts, including supplements, schedules,
19 appendices, and/or addenda thereto) in order to provide secure monitoring and
20 protection of Plaintiff's and Class members' Personal and Medical Information.

21 184. The contracts were purposefully and expressly made for the benefit
22 of Plaintiff and the Class, as it was their Personal and Medical Information that
23 Defendants agreed to collect, exchange, and protect. Thus, this benefit of
24 collection and protection of the Personal and Medical Information belonging to
25 Plaintiff and the Class was the direct and primary object of the contracting parties.

26 185. Defendants breached these promises by failing to comply with
27 HIPAA and reasonable industry practices.

1 186. As a result of Defendants’ breach of these terms, Plaintiff and the
2 Class have been seriously harmed and put at grave risk of debilitating future
3 harms.

4 187. Allowing Plaintiff and the Class to bring this claim against
5 Defendants is consistent with the objectives of the contracts and the reasonable
6 expectations of Defendants.

7 188. Plaintiff and Class members are therefore entitled to damages in an
8 amount to be determined at trial.

9 **D. COUNT IV – BREACH OF IMPLIED CONTRACT**
10 **(ALTERNATIVELY TO COUNT IV)**

11 189. Plaintiff incorporates by reference all allegations of the preceding
12 paragraphs as though fully set forth herein.

13 190. When Plaintiff and the Class members provided their Personal and
14 Medical Information to Defendants when seeking medical services, they entered
15 into implied contracts in which Defendants agreed to comply with their statutory
16 and common law duties to protect Plaintiff’s and Class members’ Personal and
17 Medical Information and to timely notify them in the event of a data breach.

18 191. Defendants required Plaintiff and Class members to provide Personal
19 and Medical Information in order to receive medical services.

20 192. Defendants affirmatively represented that they collected and stored
21 the Personal and Medical Information of Plaintiff and the members of the Class in
22 compliance with HIPAA and other statutory and common law duties using
23 reasonable, industry standard means.

24 193. Based on the implicit understanding and also on Defendants’
25 representations (as described above), Plaintiff and the Class accepted Defendants’
26 offers and provided Defendants with their Personal and Medical Information.

27 194. Plaintiff and Class members would not have provided their Personal
28 and Medical Information to Defendants had they known that Defendants would

1 not safeguard their Personal and Medical Information, as promised, or provide
2 timely notice of a data breach.

3 195. Plaintiff and Class members fully performed their obligations under
4 the implied contracts with Defendants.

5 196. Defendants breached the implied contracts by failing to safeguard
6 Plaintiff's and Class members' Personal and Medical Information and by failing to
7 provide them with timely and accurate notice of the Data Breach.

8 197. The losses and damages Plaintiff and Class members sustained (as
9 described above) were the direct and proximate result of Defendants' breach of the
10 implied contract with Plaintiff and Class members.

11 **E. COUNT V – BREACH OF CONFIDENCE**

12 198. Plaintiff incorporates by reference all allegations of the preceding
13 paragraphs as though fully set forth herein.

14 199. At all times during Plaintiff's and Class members' interactions with
15 Defendants, Defendants were fully aware of the confidential nature of the Personal
16 and Medical Information that Plaintiff and Class members provided to
17 Defendants.

18 200. As alleged herein and above, Defendants' relationship with Plaintiff
19 and the Class was governed by promises and expectations that Plaintiff and Class
20 members' Personal and Medical Information would be collected, stored, and
21 protected in confidence, and would not be accessed by, acquired by, appropriated
22 by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by,
23 and/or viewed by unauthorized third parties.

24 201. Plaintiff and Class members provided their respective Personal and
25 Medical Information to Defendants with the explicit and implicit understandings
26 that Defendants would protect and not permit the Personal and Medical
27 Information to be accessed by, acquired by, appropriated by, disclosed to,
28

1 encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by
2 unauthorized third parties.

3 202. Plaintiff and Class members also provided their Personal and Medical
4 Information to Defendants with the explicit and implicit understandings that
5 Defendants would take precautions to protect their Personal and Medical
6 Information from unauthorized access, acquisition, appropriation, disclosure,
7 encumbrance, exfiltration, release, theft, use, and/or viewing, such as following
8 basic principles of protecting their networks and data systems.

9 203. Defendants voluntarily received, in confidence, Plaintiff's and Class
10 members' Personal and Medical Information with the understanding that the
11 Personal and Medical Information would not be accessed by, acquired by,
12 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
13 by, used by, and/or viewed by the public or any unauthorized third parties.

14 204. Due to Defendants' failure to prevent, detect, and avoid the Data
15 Breach from occurring by, inter alia, not following best information security
16 practices to secure Plaintiff's and Class members' Personal and Medical
17 Information, Plaintiff's and Class members' Personal and Medical Information
18 was accessed by, acquired by, appropriated by, disclosed to, encumbered by,
19 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third
20 parties beyond Plaintiff's and Class members' confidence, and without their
21 express permission.

22 205. As a direct and proximate cause of Defendants' actions and/or
23 omissions, Plaintiff and Class members have suffered damages as alleged herein.

24 206. But for Defendants' failure to maintain and protect Plaintiff's and
25 Class members' Personal and Medical Information in violation of the parties'
26 understanding of confidence, their Personal and Medical Information would not
27 have been accessed by, acquired by, appropriated by, disclosed to, encumbered by,
28 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third

1 parties. Defendants' Data Breach was the direct and legal cause of the misuse of
2 Plaintiff's and Class members' Personal and Medical Information, as well as the
3 resulting damages.

4 207. The injury and harm Plaintiff and Class members suffered and will
5 continue to suffer was the reasonably foreseeable result of Defendants'
6 unauthorized misuse of Plaintiff's and Class members' Personal and Medical
7 Information. Defendants knew their data systems and protocols for accepting and
8 securing Plaintiff's and Class members' Personal and Medical Information had
9 security and other vulnerabilities that placed Plaintiff's and Class members'
10 Personal and Medical Information in jeopardy.

11 208. As a direct and proximate result of Defendants' breaches of
12 confidence, Plaintiff and Class members have suffered and will suffer injury, as
13 alleged herein, including but not limited to (a) actual identity theft; (b) the
14 compromise, publication, and/or theft of their Personal and Medical Information;
15 (c) out-of-pocket expenses associated with the prevention, detection, and recovery
16 from identity theft and/or unauthorized use of their Personal and Medical
17 Information; (d) lost opportunity costs associated with effort expended and the
18 loss of productivity addressing and attempting to mitigate the actual and future
19 consequences of the Data Breach, including but not limited to efforts spent
20 researching how to prevent, detect, contest, and recover from identity theft; (e) the
21 continued risk to their Personal and Medical Information, which remains in
22 Defendants' possession and is subject to further unauthorized disclosures so long
23 as Defendants fail to undertake appropriate and adequate measures to protect
24 Class members' Personal and Medical Information in their continued possession;
25 (f) future costs in terms of time, effort, and money that will be expended as result
26 of the Data Breach for the remainder of the lives of Plaintiff and Class members;
27 and (g) the diminished value of Plaintiff's and Class members Personal and
28

1 Medical Information; and (h) the diminished value of Defendants’ services
2 Plaintiff and Class members paid for and received.

3 **F. COUNT VI – BREACH OF IMPLIED COVENANT OF**
4 **GOOD FAITH AND FAIR DEALING**

5 209. Plaintiff incorporates by reference all allegations of the preceding
6 paragraphs as though fully set forth herein.

7 210. As described above, Defendants made promises and representations
8 to Plaintiff and the Class that they would comply with HIPAA and other
9 applicable laws and industry best practices.

10 211. These promises and representations became a part of the contract
11 between Defendants and Plaintiff and the Class.

12 212. While Defendants had discretion in the specifics of how they met the
13 applicable laws and industry standards, this discretion was governed by an implied
14 covenant of good faith and fair dealing.

15 213. Defendants breached this implied covenant when they engaged in
16 acts and/or omissions that are declared unfair trade practices by the FTC and state
17 statutes and regulations, and when they engaged in unlawful practices under
18 HIPAA and other state personal and medical privacy laws. These acts and
19 omissions included: representing that they would maintain adequate data privacy
20 and security practices and procedures to safeguard the Personal and Medical
21 Information from unauthorized disclosures, releases, data breaches, and theft;
22 omitting, suppressing, and concealing the material fact of the inadequacy of the
23 privacy and security protections for the Class’s Personal and Medical Information;
24 and failing to disclose to the Class at the time they provided their Personal and
25 Medical Information to them that Defendants’ data security systems and protocols,
26 including training, auditing, and testing of employees, failed to meet applicable
27 legal and industry standards.

1 214. Plaintiff and Class members did all or substantially all the significant
2 things that the contract required them to do.

3 215. Likewise, all conditions required for Defendants’ performance were
4 met.

5 216. Defendants’ acts and omissions unfairly interfered with Plaintiff’s
6 and Class members’ rights to receive the full benefit of their contracts.

7 217. Plaintiff and Class members have been harmed by Defendants’
8 breach of this implied covenant in the many ways described above, including
9 overpayment for services, imminent risk of certainly impending and devastating
10 identity theft that exists now that cyber criminals have their Personal and Medical
11 Information, and the attendant long-term time and expenses spent attempting to
12 mitigate and insure against these risks.

13 218. Defendants are liable for this breach of these implied covenants,
14 whether or not they are found to have breached any specific express contractual
15 term.

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

19 **G. COUNT VII – VIOLATIONS OF SOUTH CAROLINA CODE**
20 **OF LAWS, S.C. STAT. TIT. 39, CH. 5 §§ 10, *ET SEQ.***

21 220. Plaintiff incorporates by reference all allegations of the preceding
22 paragraphs as though fully set forth herein.

23 221. Plaintiff brings this Count against Defendants on behalf of the
24 CareSouth Subclass.

25 222. Defendants are “persons,” as defined by S.C. Stat. § 39-5-10(a).

26 223. Defendants offer, sell, and distribute goods, services, and property,
27 tangible or intangible, real, personal or mixed, and engage in trade and commerce
28

1 that directly or indirectly affects the people of South Carolina. S.C. Stat. § 39-5-
2 10(b).

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

9 225. Defendants' unlawful, unfair, and deceptive practices include:

- 10 a. Failing to implement and maintain reasonable security and
11 privacy measures to protect Plaintiff's and Class members'
12 Personal and Medical Information, which was a direct and
13 proximate cause of the Data Breach;
- 14 b. Failing to identify foreseeable security and privacy risks,
15 remediate identified security and privacy risks, and adequately
16 improve security and privacy measures following previous data
17 incidents in the healthcare industry, which was a direct and
18 proximate cause of the Data Breach;
- 19 c. Failing to comply with common law and statutory duties
20 pertaining to the security and privacy of Plaintiff's and Class
21 members' Personal and Medical Information, including duties
22 imposed by the FTC Act and HIPAA;
- 23 d. Misrepresenting that they would protect the privacy and
24 confidentiality of Plaintiff's and Class members' Personal and
25 Medical Information, including by implementing and maintaining
26 reasonable security measures;
- 27 e. Misrepresenting that they would comply with common law and
28 statutory duties pertaining to the security and privacy of Plaintiff's

1 and Class members' Personal and Medical Information, including
2 duties imposed by the FTC Act and HIPAA;

3 f. Omitting, suppressing, and concealing the material fact that they
4 did not reasonably or adequately secure Plaintiff's and Class
5 members' Personal and Medical Information; and

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

11 226. Defendants' representations and omissions were material because they
12 were likely to deceive reasonable patient consumers about the adequacy of
13 Defendants' data security and ability to protect the confidentiality of their Personal
14 and Medical Information.

15 227. Defendants intended to mislead Plaintiff and Class members and
16 induce them to rely on their misrepresentations and omissions.

17 228. Had Defendants disclosed to Plaintiff and Class members that their
18 data security protocols and business emails (where highly sensitive personal data
19 was exchanged and stored) were not secure and, thus, vulnerable to attack,
20 Defendants would not have been able to continue in business and they would have
21 been forced to adopt reasonable data security measures and comply with the law.

22 229. The above unlawful practices and acts by Defendants were immoral,
23 unethical, oppressive, unscrupulous, and substantially injurious. These acts caused
24 substantial and continuous injury to Plaintiff and Class members.

25 230. Defendants acted intentionally, knowingly, and maliciously to violate
26 South Carolina's consumer protection statute, and recklessly disregarded Plaintiff's
27 and the Class members' rights.

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

7 232. Plaintiff and CareSouth Subclass members therefore seek all monetary
8 and non-monetary relief allowed by law under S.C. Stat. § 39-5-10 *et seq.* for
9 Defendants’ violations alleged herein, including actual damages, civil penalties, and
10 attorneys’ fees and costs.

11 **H. COUNT VIII – VIOLATIONS OF SOUTH CAROLINA**
12 **CODE OF LAWS, S.C. STAT., TIT. 39, CH. 1 § 90**

13 233. Plaintiff incorporates by reference all allegations of the preceding
14 paragraphs as though fully set forth herein.

15 234. Plaintiff brings this Count against Defendants on behalf of the
16 CareSouth Subclass.

17 235. Defendants are required to disclose to members of the CareSouth
18 Subclass a data breach following discovery or notification of the breach in the
19 security of the data, and such disclosure must be made “in the most expedient time
20 possible and without unreasonable delay, consistent with ... measures necessary to
21 determine the scope of the breach and restore reasonable integrity to the data
22 system.” S.C. Stat. § 39-1-90(A).

23 236. Defendants conduct their businesses in South Carolina and own or
24 license computerized data or other data that includes personal identifying
25 information as set forth under S.C. Stat. § 39-1-90(A).

26 237. Plaintiff’s and CareSouth Subclass members’ Personal and Medical
27 Information (*e.g.*, Social Security numbers) include personal information as covered
28 under S.C. Stat. § 39-1-90(D)(3)(a).

1 238. Because Defendants were aware of the Data Breach (which caused or
2 was reasonably likely to have caused the Personal and Medical Information to be
3 acquired by unauthorized cybercriminals), Defendants had an obligation to disclose
4 the Data Breach in a timely and expedient fashion or, at a minimum, in accordance
5 with their own notification procedures, but failed in this obligation.

6 239. As a direct and proximate result of Defendants' violations of S.C. Stat.
7 § 39-1-90, Plaintiff and CareSouth Subclass members suffered damages, as
8 described herein.

9 240. Plaintiff seeks relief under S.C. Stat. § 39-1-90(G), including actual
10 damages, injunctive relief, and attorney fees, costs and expenses.

11 **I. COUNT IX – DECLARATORY RELIEF**

12 241. Plaintiff incorporates by reference all allegations of the preceding
13 paragraphs as though fully set forth herein.

14 242. Plaintiff brings this Count under the federal Declaratory Judgment
15 Act, 28 U.S.C. §2201.

16 243. As previously alleged, Plaintiff and members of the Class were either
17 third-party beneficiaries of contracts entered into between Defendants that
18 expressly required Defendants to provide the benefit of adequate security for the
19 Personal and Medical Information it collected from Plaintiff and the Class or,
20 alternatively, were parties of an implied contract with Defendants that required
21 Defendants to provide adequate security for the Personal and Medical Information
22 it collected from them.

23 244. Defendants owe a duty of care to Plaintiff and the members of the
24 Class requiring Defendants to adequately secure Personal and Medical
25 Information.

26 245. Defendants still possess Plaintiff's and Class members' Personal and
27 Medical Information.

28

1 246. Since the Data Breach, Defendants have announced few if any
2 changes to their data security infrastructure, processes or procedures to fix the
3 vulnerabilities in their computer systems and/or security practices that permitted
4 the Data Breach to occur and go undetected for months.

5 247. Defendants have not satisfied their contractual obligations and legal
6 duties to Plaintiff and the Class. In fact, now that Defendants' insufficient data
7 security and payment of the requested ransom is known to hackers, the Personal
8 and Medical Information in Defendants' possession is even more vulnerable to
9 subsequent and continuous cyberattacks.

10 248. Actual harm has arisen in the wake of the Data Breach regarding
11 Defendants' contractual obligations and duties of care to provide security
12 measures to Plaintiff and the members of the Class. Further, Plaintiff and members
13 of the Class are at risk of additional or further harm due to the nature of the
14 ransomware attack at issue, the exposure of their Personal and Medical
15 Information, and Defendants' failure to address the security failings that led to
16 such exposure.

17 249. There is no reason to believe that Defendants' security measures are
18 any more adequate now than they were before the Data Breach to meet
19 Defendants' contractual obligations and legal duties.

20 250. Plaintiff, therefore, seeks a declaration that Defendants' existing
21 security measures do not comply with their contractual obligations and duties of
22 care to provide adequate security and that, to comply with their contractual
23 obligations and duties of care, Defendants must implement and maintain
24 additional security measures.

25 **VII. PRAYER FOR RELIEF**

26 WHEREFORE, Plaintiff and the Class pray for judgment against
27 Defendants as follows:
28

- 1 a. An order certifying this action as a class action under Fed. R.
2 Civ. P. 23, defining the Class as requested herein, appointing
3 the undersigned as Class counsel, and finding that Plaintiff is a
4 proper representative of the Class requested herein;
- 5 b. A judgment in favor of Plaintiff and the Class awarding them
6 appropriate monetary relief, including actual and statutory
7 damages, punitive damages, attorney fees, expenses, costs, and
8 such other and further relief as is just and proper.
- 9 c. An order providing injunctive and other equitable relief as
10 necessary to protect the interests of the Class and the general
11 public as requested herein, including, but not limited to:
- 12 i. Ordering that Defendants engage third-party security
13 auditors/penetration testers as well as internal security
14 personnel to conduct testing, including simulated
15 attacks, penetration tests, and audits on Defendants'
16 systems on a periodic basis, and ordering Defendants to
17 promptly correct any problems or issues detected by
18 such third-party security auditors;
- 19 ii. Ordering that Defendants engage third-party security
20 auditors and internal personnel to run automated security
21 monitoring;
- 22 iii. Ordering that Defendants audit, test, and train their
23 security personnel regarding any new or modified
24 procedures;
- 25 iv. Ordering that Defendants segment customer data by,
26 among other things, creating firewalls and access
27 controls so that if one area of Defendants' systems is
28

1 compromised, hackers cannot gain access to other
2 portions of Defendants’ systems;

3 v. Ordering that Defendants purge, delete, and destroy in a
4 reasonably secure manner customer data not necessary
5 for their provisions of services;

6 vi. Ordering that Defendants conduct regular database
7 scanning and securing checks;

8 vii. Ordering that Defendants routinely and continually
9 conduct internal training and education to inform
10 internal security personnel how to identify and contain a
11 breach when it occurs and what to do in response to a
12 breach; and

13 viii. Ordering Defendants to meaningfully educate their
14 current, former, and prospective employees and
15 subcontractors about the threats they face as a result of
16 the loss of their financial and personal information to
17 third parties, as well as the steps they must take to
18 protect themselves;

19 d. An order requiring Defendants to pay the costs involved in
20 notifying the Class members about the judgment and
21 administering the claims process;

22 e. A judgment in favor of Plaintiff and the Class awarding them
23 pre-judgment and post-judgment interest, reasonable attorneys’
24 fees, costs and expenses as allowable by law; and

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

27 /////

28 /////

1 **VIII. DEMAND FOR JURY TRIAL**

2 Plaintiff demands a trial by jury on all issues so triable.

3 DATED: August 10, 2021

GREEN & NOBLIN, P.C.

4
5 By: s/Robert S. Green
6 Robert S. Green

7 James Robert Noblin
8 Emrah M. Sumer
9 2200 Larkspur Landing Circle, Ste. 101
10 Larkspur, CA 94939
11 Telephone: (415) 477-6700
12 Facsimile: (415) 477-6710

13 *Counsel for Plaintiff and the*
14 *Proposed Class*

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

Chaya Clark, individually and on behalf of all others similarly situated and on behalf of the general public

(b) County of Residence of First Listed Plaintiff Dillon County, SC (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Robert S. Green, GREEN & NOBLIN, P.C. 2200 Larkspur Landing Circle, Suite 101, Larkspur California 94939 (415) 477-6700

DEFENDANTS

Netgain Technology, LLC, and CareSouth Carolina, Inc.

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

'21CV1432 DMS BLM

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status. Includes options for Citizen of This State, Citizen of Another State, and Citizen or Subject of a Foreign Country.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

Large table with categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Each category contains a list of specific legal claims with checkboxes.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding, 2 Removed from State Court, 3 Remanded from Appellate Court, 4 Reinstated or Reopened, 5 Transferred from Another District (specify), 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)

Brief description of cause: Claims arising out of data breach that released personal and medical information

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ CHECK YES only if demanded in complaint: JURY DEMAND: [X] Yes [] No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE August 10, 2021 SIGNATURE OF ATTORNEY OF RECORD /s/ Robert S. Green

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT 1



C/O IDX
PO Box 4129
Everett WA 98204

*****AUTO**5-DIGIT 29536



Chaya Clark
721 Highway 501 S Apt 4D
Latta SC 29565-4548

49246
0970111
Ver 1A12

To Enroll, Please Call:
(833) 664-2012
Or Visit:
<https://response.idx.us/caresouth-netgain-incident>
Enrollment Code: 2XNZGT9ZX5

May 17, 2021

Notice of Data Breach

Dear Chaya Clark,

At CareSouth Carolina, we take seriously our responsibility to protect the privacy and security of your personal information. We are writing to tell you about an incident that involved personal information maintained by our vendor, Netgain Technology, Inc. ("Netgain"). Netgain provides online data storage and other services for CareSouth Carolina.

What Happened

On December 1, 2020, Netgain informed CareSouth Carolina that it was investigating an IT security incident. At that time, CareSouth Carolina had no reason to believe that patient information was involved. On January 14, 2021, Netgain informed CareSouth Carolina that its investigation found that some of servers that it maintained for CareSouth Carolina were affected as part of a ransomware attack on December 3, 2020. On April 13, 2021, CareSouth Carolina received a copy of the records that Netgain believed were affected by the attack. On April 27, 2021, CareSouth Carolina completed its review of the records and determined that your information was involved.

What Information Was Involved

CareSouth Carolina determined that the following information was not involved in this incident: your financial information (credit card and bank account numbers). CareSouth Carolina determined that the following information was involved in this incident: your name, date of birth, address, diagnosis/conditions, lab results, medications and other clinical information. For a small number of patients, Social Security numbers were involved.

What CareSouth Carolina Is Doing

In response to this incident, we required our employees to change their passwords for the affected systems and we are implementing additional security software for our networks. We also reported this incident to the federal government and to consumer reporting agencies.

We are also offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Netgain Is Doing

Netgain reported this incident to law enforcement and worked with cybersecurity experts to address, contain and recover from this incident. Netgain also paid a significant amount to the attacker in exchange for promises that the attacker will delete all copies of the data and that it will not publish, sell, or otherwise share the data. In addition, Netgain's

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Netgain, CareSouth Face Class Action Over Dec. 2020 Ransomware Attack](#)
