

1 Bibianne U. Fell (SBN 234194)
2 **FELL LAW, P.C.**
3 Mailing: 11956 Bernardo Plaza Dr., Box 531
4 San Diego, CA 92128
5 **Personal Service:** 402 W. Broadway, Suite 950
6 San Diego, CA 92101
7 Telephone: (858) 201-3960
8 Facsimile: (858) 201-3966
9 *bibi@fellfirm.com*

6 William B. Federman*
7 Oklahoma Bar No. 2853
8 **FEDERMAN & SHERWOOD**
9 10205 N. Pennsylvania Ave.
10 Oklahoma City, OK 73120
11 Telephone: (405) 235-1560
12 Facsimile: (405) 239-2112
13 *wbf@federmanlaw.com*

11 **Pro Hac Vice* application to be submitted

12 *Counsel for Plaintiff and the Proposed Class*

13 **UNITED STATES DISTRICT COURT**
14 **SOUTHERN DISTRICT OF CALIFORNIA**

15 Kate Rasmuzzen, individually and on
16 behalf of all others similarly situated
17 and on behalf of the general public,

18 Plaintiff,

19 v.

20 Scripps Health

21 Defendant.

Case No.: '21CV1143 H DEB

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff, Kate Rasmuzzen (“Ms. Rasmuzzen” or “Plaintiff Rasmuzzen”),
2 individually and on behalf of all others similarly situated and on behalf of the
3 general public, for her Class Action Complaint, brings this action against
4 Defendant Scripps Health (“Scripps”) based on personal knowledge and the
5 investigation of counsel and alleges as follows:

6 **I. INTRODUCTION**

7 1. With this action, Plaintiff seeks to hold Defendant responsible for the
8 harms it caused Plaintiff and the over one hundred forty-seven thousand (147,000)
9 of other similarly situated persons in the massive and preventable ransomware
10 attack that took place on or around April 29, 2021, by which cyber criminals
11 infiltrated Defendant’s inadequately protected network servers where highly
12 sensitive personal and medical information was being kept unprotected (“Data
13 Breach” or “Breach”).¹

14 2. The cybercriminals gained access to certain of Defendant’s network
15 servers with the apparent intention of profiting from such access.

16 3. Defendant Scripps is the second largest healthcare provider in San
17 Diego.² On its website, Scripps touts that it “takes great care to ensure [its
18 patients’] health information is kept private and secure.”³

19 4. Plaintiff and Class members were required, as patients of Scripps, to
20 provide Defendant with their “Personal and Medical Information” (defined
21 below), with the assurance that such information would be kept safe from
22 unauthorized access. By taking possession and control of Plaintiff’s and Class
23 members’ Personal and Medical Information, Defendant assumed a duty to
24

25 ¹ See <https://www.hipaajournal.com/147000-patients-affected-by-scripps-health-ransomware-attack/#:~:text=Scripps%20Health%2C%20the%20second%20largest,May%201%2C%202021%20ransomware%20attack> (last accessed June 18, 2021).

26 ² *Id.*

27 ³ See <https://www.scripps.org/patients-and-visitors/medical-records> (last accessed
28 June 18, 2021).

1 securely store and protect the Personal and Medical Information of Plaintiff and
2 the Class.

3 5. Defendant breached this duty and betrayed the trust of Plaintiff and
4 Class members by failing to properly safeguard and protect their Personal and
5 Medical Information, thus enabling cybercriminals to access, acquire, appropriate,
6 compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

7 6. The Personal and Medical Information compromised includes names,
8 addresses, dates of birth, health insurance information, medical record numbers,
9 patient account numbers, clinical information, dates of service, treatment
10 information, Social Security numbers, and/or driver's license numbers.⁴

11 7. Defendant's misconduct – failing to timely implement adequate and
12 reasonable measures to protect Plaintiff's Personal and Medical Information,
13 failing to timely detect the Data Breach, failing to take adequate steps to prevent
14 and stop the Data Breach, failing to disclose the material facts that they did not
15 have adequate security practices in place to safeguard the Personal and Medical
16 Information, and failing to honor their promises and representations to protect
17 Plaintiff's and Class members' Personal and Medical Information – caused
18 substantial harm and injuries to Plaintiff and Class members across the United
19 States.

20 8. Due to Defendant's negligence and data security failures, cyber
21 criminals obtained and now possess everything they need to commit personal and
22 medical identity theft and wreak havoc on the financial and personal lives of
23 hundreds of thousands of individuals for decades to come.

24 9. As a result of the Data Breach, Plaintiff and Class members have
25 already suffered damages. For example, now that their Personal and Medical
26 Information has been released into the criminal cyber domains, Plaintiff and Class
27

28 ⁴ See Sample Notice Letter, <https://oag.ca.gov/system/files/Scripps%20Health-%20Sample%20Notice.pdf> (last accessed June 18, 2021).

1 members are at imminent and impending risk of identity theft. This risk will
2 continue for the rest of their lives, as Plaintiff and Class members are now forced
3 to deal with the danger of identity thieves possessing and using their Personal and
4 Medical Information. Additionally, Plaintiff and Class members have already lost
5 time and money responding to and mitigating the impact of the Data Breach,
6 which efforts are continuous and ongoing.

7 10. Plaintiff brings this action individually and on behalf of the Class and
8 seeks actual damages, statutory damages, punitive damages, and restitution, with
9 attorney fees, costs, and expenses, under the California Confidentiality of Medical
10 Information Act (“CMIA”), Cal. Civ. Code § 56, *et seq.*, California’s Unfair
11 Competition Law (“UCL”), Cal. Bus. Prof. Code § 17200, *et seq.*, and further sues
12 Defendant for, among other causes of action, negligence (including negligence *per*
13 *se*). Plaintiff also seeks declaratory and injunctive relief, including significant
14 improvements to Defendant’s data security systems and protocols, future annual
15 audits, Defendant-funded long-term credit monitoring services, and other remedies
16 as the Court sees necessary and proper.

17 **II. THE PARTIES**

18 11. Plaintiff Kate Rasmuzzen is a citizen and resident of the State of
19 California.

20 12. Ms. Rasmuzzen was a patient of, and received medical services from,
21 Scripps. Her Personal and Medical Information was within the possession and
22 control of Defendant at the time of the Data Breach.

23 13. Plaintiff received a letter from Scripps dated June 1, 2021, informing
24 her that her Personal and Medical Information was involved in the Data Breach.
25 *See Exhibit 1*, the “Notice.”

26 14. As required in order to obtain medical services from Scripps, Plaintiff
27 provided Scripps with highly sensitive personal, financial, health, and insurance
28 information.

1 15. Because of Defendant’s negligence leading up to and including the
2 period of the Data Breach, Plaintiff’s Personal and Medical Information is now in
3 the hands of cyber criminals and Plaintiff is under an imminent and substantially
4 likely risk of identity theft and fraud, including medical identity theft and medical
5 fraud.

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

14 17. As a direct and proximate result of the Data Breach, Plaintiff and the
15 Class will be required to purchase a yearly subscription to identity theft protection,
16 which Defendant failed to provide to them. The purchase of identity theft
17 protection and credit monitoring will be necessary in order to protect themselves
18 from medical identity theft and other types of fraud, of which they are now
19 substantially at risk. This subscription will need to be renewed yearly for the rest
20 of their lives.

21 18. Plaintiff and Class members have also suffered injury directly and
22 proximately caused by the Data Breach, including damages and diminution in
23 value of their Personal and Medical Information that was entrusted to Defendant
24 for the sole purpose of obtaining medical services necessary for their health and
25 well-being, with the understanding that Defendant would safeguard this
26 information against disclosure. Additionally, Plaintiff’s and Class members’
27 Personal and Medical Information is at continued risk of compromise and
28 unauthorized disclosure as it remains in the possession the cybercriminals who

1 carried out the Data Breach and of Defendant, and is thus subject to further
2 breaches so long as Defendant fails to undertake appropriate and adequate
3 measures to protect it.

4 19. Defendant Scripps is the second largest healthcare provider in San
5 Diego and is a “\$3.1 billion not-for-profit health care organization whose legacy
6 spans decades for one shining reason – excellence.”⁵

7 20. As part of its business, Defendant collects substantial amounts of
8 Personal and Medical Information. The medical information that Defendant
9 collects qualifies as “Medical Information” under the federal Health Information
10 Portability and Accountability Act (“HIPAA”), the CMIA, and other state medical
11 record protection acts.

12 **III. JURISDICTION AND VENUE**

13 21. This Court has diversity jurisdiction over this action under the Class
14 Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action
15 involving more than 100 class members, the amount in controversy exceeds
16 \$5,000,000, exclusive of interest and costs and, upon information and belief, the
17 Class includes members who are citizens of states that differ from Defendant.

18 22. This Court has personal jurisdiction over Defendant because
19 Defendant Scripps conducts much of its business in and has sufficient minimum
20 contacts with California.

21 23. Venue is likewise proper as to Defendant in this District under 28
22 U.S.C. § 1391(a)(1) because Defendant Scripps’s headquarters are located in this
23 District and it conducts much of its business through this District (including
24 promoting, selling, marketing, and distributing the Scripps brand and services at
25 issue).

26 ///

27 ///

28 _____
⁵ See <https://www.scripps.org/about-us> (last accessed June 18, 2021).

1 **IV. FACTUAL ALLEGATIONS**

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

3 24. On or about April 29, 2021, Defendant Scripps’s network servers
4 were subject to a ransomware attack through which unauthorized third-party
5 cybercriminals gained access to Plaintiff’s and Class members’ Personal and
6 Medical Information.

7 25. Scripps sent a sample notice of data breach letter that mirrored the
8 language of the Notice sent to Plaintiff and Class members.

9 26. Pursuant to California Civ. Code § 1798.82(f), “[a] person or
10 business that is required to issue a security breach notification pursuant to
11 [§ 1798.82(a)] to more than 500 California residents as a result of a single breach
12 of the security system shall electronically submit a single sample copy of that
13 security breach notification, excluding any personally identifiable information, to
14 the Attorney General.”

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

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

21 29. California Civ. Code § 1798.82(g) defines “breach of the security of
22 the system” as the “unauthorized acquisition of computerized data that
23 compromises the security, confidentiality, or integrity of personal information
24 maintained by the person or business.”

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

27 ///

28 ///

1 31. Plaintiff’s and Class members’ unencrypted personal information was
2 acquired by an unauthorized cybercriminal or cybercriminals as a result of the
3 Data Breach.

4 32. Defendant reasonably believe Plaintiff’s and Class members’
5 unencrypted personal information was acquired by an unauthorized person as a
6 result of the Data Breach.

7 33. The security, confidentiality, or integrity of Plaintiff’s and Class
8 members’ unencrypted personal information was compromised as a result of the
9 Data Breach.

10 34. Defendant reasonably believed the security, confidentiality, or
11 integrity of Plaintiff’s and Class members’ unencrypted personal information was
12 compromised as a result of the Data Breach.

13 35. Plaintiff’s and Class members’ unencrypted personal information that
14 was acquired by an unauthorized person as a result of the Data Breach was viewed
15 by unauthorized persons.

16 36. Defendant reasonably believed Plaintiff’s and Class members’
17 unencrypted personal information that was acquired by an unauthorized person as
18 a result of the Data Breach was viewed by unauthorized persons.

19 37. It is reasonable to infer that Plaintiff’s and Class members’
20 unencrypted personal information that was acquired by an unauthorized person as
21 a result of the Data Breach was viewed by unauthorized persons.

22 38. It should be presumed that Plaintiff’s and Class members’
23 unencrypted personal information that was acquired by an unauthorized person as
24 a result of the Data Breach was viewed by unauthorized persons.

25 39. After receiving letters similar to those sent pursuant to California Civ.
26 Code § 1798.82(a)(1) – and filed with the Attorney General of California in
27 accordance with California Civ. Code § 1798.82(f) – it is reasonable for
28 recipients, including Plaintiff and Class members in this case, to (i) believe that

1 the risk of future harm (including identity theft) is real and imminent, and (ii) take
2 steps to mitigate that risk of future harm.

3 **B. The Data Breach and Defendant’s Failed Response**

4 40. It is apparent from the various notices and sample notices of the Data
5 Breach sent to Plaintiff, the Class, and state Attorneys General that the Personal
6 and Medical Information contained on Defendant’s servers was not encrypted.

7 41. Following discovery of the Data Breach, Defendant began to
8 investigate and address the Data Breach. Based upon the investigation, the
9 attackers were able to access certain network servers containing the Personal and
10 Medical Information at issue, which was being held, unencrypted and unprotected.

11 42. Upon information and belief, the unauthorized third-party
12 cybercriminals gained access to the Personal and Medical Information with the
13 intent of engaging in misuse of the Personal and Medical Information, including
14 marketing and selling Plaintiff’s and Class members’ Personal and Medical
15 Information on the dark web.

16 43. In spite of the severity of the Data Breach, Defendant has done very
17 little to protect Plaintiff and the Class. For example, in the Notice, Defendant only
18 provides twelve (12) months of identity theft and credit monitoring protection to a
19 select few Data Breach victims.

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

24 45. The Notice fails to provide the consolation Plaintiff and Class
25 members seek and certainly falls far short of eliminating the substantial risk of
26 fraud and identity theft Plaintiff and the Class now face.

27 ///

28 ///

1 46. Ransomware creators, such as the authors of Defendant’s Data
2 Breach, “are criminals without any ethics,” so there is no guarantee they will do
3 what they promise to do in exchange for any ransom money they receive.⁶

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

10 48. Moreover, paying the ransom (if Scripps did indeed pay the ransom)
11 will only encourage attackers to carry out these types of cyberattacks on Scripps’s
12 system networks in the future.

13 49. Defendant failed to adequately safeguard Plaintiff’s and Class
14 members’ Personal and Medical Information, allowing cyber criminals to access
15 this wealth of priceless information, with virtually no offer of remedy or relief
16 while failing to spend sufficient resources on cybersecurity training and adequate
17 data security measures and protocols.

18 50. Defendant had obligations created by HIPAA, the CMIA, reasonable
19 industry standards, common law, state statutory law, and its own assurances and
20 representations to keep patients’ Personal and Medical Information confidential
21 and to protect such Personal and Medical Information from unauthorized access.

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

26
27
28 ⁶ <https://enterprise.comodo.com/does-paying-ransomware-work.php> (last accessed June 10, 2021).

1 52. The stolen Personal and Medical Information at issue has great value
2 to the ransomware attackers, due to the large number of individuals affected and
3 the fact that health insurance information, clinical information, driver’s license
4 numbers, and Social Security numbers were part of the data that was
5 compromised.

6 **C. Defendant had an Obligation to Protect Personal and Medical**
7 **Information under Federal Law and the Applicable Standard of**
8 **Care**

9 53. Defendant is covered by HIPAA (45 C.F.R. § 160.102). As such, it is
10 required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.
11 Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually
12 Identifiable Health Information”), and Security Rule (“Security Standards for the
13 Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and
14 Part 164, Subparts A and C.

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

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

22 56. HIPAA requires Defendant to “comply with the applicable standards,
23 implementation specifications, and requirements” of HIPAA “with respect to
24 electronic protected health information.” 45 C.F.R. § 164.302.

25 57. “Electronic protected health information” is “individually identifiable
26 health information ... that is (i) transmitted by electronic media; maintained in
27 electronic media.” 45 C.F.R. § 160.103.

28 58. HIPAA’s Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by their workforce.

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

60. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”⁷

61. Defendant was 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).

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

10 63. Defendant owed a duty to Plaintiff and the Class to design, maintain,
11 and test its computer systems and networks to ensure that the Personal and
12 Medical Information in its possession was adequately secured and protected.

13 64. Defendant owed a duty to Plaintiff and the Class to create and
14 implement reasonable data security practices and procedures to protect the
15 Personal and Medical Information in its possession.

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

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

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

26 68. Defendant owed a duty of care to Plaintiff and the Class because they
27 were foreseeable and probable victims of any inadequate data security practices.
28

1 **D. Defendant was on Notice of Cyber Attack Threats in the**
2 **Healthcare Industry and of the Inadequacy of its Data Security**

3 69. Defendant was on notice that companies in the healthcare industry
4 were targets for cyberattacks.

5 70. Defendant was on notice that the FBI has recently been concerned
6 about data security in the healthcare industry. In August 2014, after a cyberattack
7 on Community Health Systems, Inc., the FBI warned companies within the
8 healthcare industry that hackers were targeting them. The warning stated that
9 “[t]he FBI has observed malicious actors targeting healthcare related systems,
10 perhaps for the purpose of obtaining the Protected Healthcare Information (PHI)
11 and/or Personally Identifiable Information (PII).”⁸

12 71. The American Medical Association (“AMA”) has also warned
13 healthcare companies about the importance of protecting their patients’
14 confidential information:

15 Cybersecurity is not just a technical issue; it’s a patient safety
16 issue. AMA research has revealed that 83% of physicians
17 work in a practice that has experienced some kind of
18 cyberattack. Unfortunately, practices are learning that
19 cyberattacks not only threaten the privacy and security of
20 patients’ health and financial information, but also patient
21 access to care.⁹

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

26 ⁸ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*,
REUTERS (Aug. 2014), <http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>.

27 ⁹ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics,*
28 *hospitals*, AM. MED. ASS’N (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>.

1 73. Defendant was on notice that the federal government has been
2 concerned about healthcare company data encryption. Defendant knew it kept
3 protected health information on its servers and yet it appears Defendant did not
4 encrypt this information.

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

13 75. As a covered entity under HIPAA, Defendant should have known its
14 systems were prone to ransomware and other types of cyberattacks and sought
15 better protection for the Personal and Medical Information accumulating in its
16 system networks.

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

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

23 77. Each year, identity theft causes tens of billions of dollars of losses to
24 victims in the United States.¹¹ For example, with the Personal and Medical

25 ¹⁰“Stolen Laptops Lead to Important HIPAA Settlements,” U.S. Dep’t of Health
26 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](https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html).

27 ¹¹“Facts + Statistics: Identity Theft and Cybercrime,” Insurance Info. Inst.,
28 <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”).

1 Information stolen in the Data Breach, including Social Security numbers and
2 driver's licenses, identity thieves can open financial accounts, apply for credit, file
3 fraudulent tax returns, commit crimes, create false driver's licenses and other
4 forms of identification and sell them to other criminals or undocumented
5 immigrants, steal government benefits, give breach victims' names to police
6 during arrests, and many other harmful forms of identity theft.¹² These criminal
7 activities have and will result in devastating financial and personal losses to
8 Plaintiff and Class members.

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

12 79. For example, it is believed that certain Personal and Medical
13 Information compromised in the 2017 Experian data breach was being used, three
14 years later, by identity thieves to apply for COVID-19-related benefits in the state
15 of Oklahoma.¹⁴

16 80. This was a financially motivated Data Breach, as apparent from the
17 ransom money sought by the cyber criminals, who will continue to seek to profit
18 off of the sale of Plaintiff's and the Class members' Personal and Medical
19 Information on the dark web. The Personal and Medical Information exposed in
20 this Data Breach is valuable to identity thieves for use in the kinds of criminal
21 activity described herein.

24 ¹²See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social*
25 *Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

26 ¹³*Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007,
27 <https://www.gao.gov/assets/270/262904.html>

28 ¹⁴See <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 81. These risks are both certainly impending and substantial. As the FTC
2 has reported, if hackers get access to personally identifiable information, they will
3 use it.¹⁵

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

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

12 83. For instance, with a stolen Social Security number, which is part of
13 the Personal and Medical Information compromised in the Data Breach, someone
14 can open financial accounts, get medical care, file fraudulent tax returns, commit
15 crimes, and steal benefits.¹⁷ Identity thieves can also use the information stolen
16 from Plaintiff and Class members to qualify for expensive medical care and leave
17 them and their contracted health insurers on the hook for massive medical bills.

18 84. Medical identity theft is one of the most common, most expensive,
19 and most difficult-to-prevent forms of identity theft. According to Kaiser Health
20 News, “medical-related identity theft accounted for 43 percent of all identity thefts
21 reported in the United States in 2013,” which is more than identity thefts involving
22 banking and finance, the government and the military, or education.¹⁸

23
24
25 ¹⁵Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N
(May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

26 ¹⁶*Data Breaches Are Frequent*, *supra* note 11.

27 ¹⁷*See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

28 ¹⁸Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

1 85. “Medical identity theft is a growing and dangerous crime that leaves
2 its victims with little to no recourse for recovery,” reported Pam Dixon, executive
3 director of World Privacy Forum. “Victims often experience financial
4 repercussions and worse yet, they frequently discover erroneous information has
5 been added to their personal medical files due to the thief’s activities.”¹⁹

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

14 87. If cyber criminals manage to access financial information, health
15 insurance information, and other personally sensitive data—as they did here—
16 there is no limit to the amount of fraud to which Defendant may expose the
17 Plaintiff and Class members.

18 88. A study by Experian found that the average total cost of medical
19 identity theft is “about \$20,000” per incident, and that a majority of victims of
20 medical identity theft were forced to pay out-of-pocket costs for healthcare they
21 did not receive in order to restore coverage.²² Almost half of medical identity
22

23 ¹⁹ *Id.*

24 ²⁰ IDExperts, *You Got It, They Want It: Criminals Targeting Your Private*
25 *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>.

26 ²¹ *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS:
27 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>.

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

1 theft victims lose their healthcare coverage as a result of the incident, while nearly
2 one-third saw their insurance premiums rise, and forty percent were never able to
3 resolve their identity theft at all.²³

4 89. As described above, identity theft victims must spend countless hours
5 and large amounts of money repairing the impact to their credit.²⁴

6 90. Defendant’s failure to offer identity monitoring to the most members
7 of the Class, including to Plaintiff, is egregious. Moreover, Defendant’s offer of
8 one year of identity theft monitoring to a few members of the Class is woefully
9 inadequate, as the worst is yet to come.

10 91. Victims of the Data Breach, like Plaintiff and other Class members,
11 must spend many hours and large amounts of money protecting themselves from
12 the future negative impacts to their credit because of the Data Breach.²⁵

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

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

26 ²⁴ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4
27 (Sept. 2013), [http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf)
28 [theft-victims.pdf](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf).

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

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

- 3 a. Trespass and damage their personal property, including
4 Personal and Medical Information;
- 5 b. Improper disclosure of their Personal and Medical Information;
- 6 c. The imminent and certainly impending injury flowing from
7 potential fraud and identity theft posed by their Personal and
8 Medical Information being placed in the hands of criminals;
- 9 d. The imminent and certainly impending risk of having their
10 confidential medical information used against them by spam
11 callers to defraud them;
- 12 e. Loss of privacy suffered as a result of the Data Breach;
- 13 f. Ascertainable losses in the form of the value of their time
14 reasonably expended to remedy or mitigate the effects of the
15 Data Breach;
- 16 g. Ascertainable losses in the form of deprivation of the value of
17 patients' personal information, for which there is a well-
18 established and quantifiable national and international market;
19 and
- 20 h. The loss of use of and access to their credit, accounts, and/or
21 funds.

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

28 ///

1 95. Plaintiff and Class members are desperately trying to mitigate the
2 damage that Defendant has caused them but, given the kind of Personal and
3 Medical Information Defendant made accessible to hackers, they are certain to
4 incur additional damages. Because identity thieves have their Personal and
5 Medical Information, Plaintiff and all Class members will need to have identity
6 theft monitoring protection for the rest of their lives. Some may even need to go
7 through the long and arduous process of getting a new Social Security number,
8 with all the loss of credit and employment difficulties that come with this
9 change.²⁶

10 96. None of this should have happened. The Data Breach was
11 preventable.

12 **F. Defendant Could Have Prevented the Data Breach but Failed to**
13 **Adequately Protect Plaintiff’s and Class Members’ Personal and**
14 **Medical Information**

15 97. Data breaches are preventable.²⁷ As Lucy Thompson wrote in the
16 DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data
17 breaches that occurred could have been prevented by proper planning and the
18 correct design and implementation of appropriate security solutions.”²⁸ She added
19 that “[o]rganizations that collect, use, store, and share sensitive personal data must
20 accept responsibility for protecting the information and ensuring that it is not
21 compromised”²⁹

22 98. “Most of the reported data breaches are a result of lax security and
23 the failure to create or enforce appropriate security policies, rules, and procedures
24 ... Appropriate information security controls, including encryption, must be

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

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

28 ²⁸*Id.* at 17.

29 ²⁹*Id.* at 28.

1 implemented and enforced in a rigorous and disciplined manner so that a *data*
2 *breach never occurs.*”³⁰

3 99. Defendant required Plaintiff and Class members to surrender their
4 Personal and Medical Information – including but not limited to their names,
5 addresses, driver’s licenses, Social Security numbers, medical information, and
6 health insurance information – and was entrusted with properly holding,
7 safeguarding, and protecting against unlawful disclosure of such Personal and
8 Medical Information.

9 100. Many failures laid the groundwork for the success (“success” from
10 the cybercriminals’ viewpoint) of the Data Breach, starting with Defendant’s
11 failure to incur the costs necessary to implement adequate and reasonable cyber
12 security protections, procedures and protocols necessary to safeguard Plaintiff’s
13 and Class members’ Personal and Medical Information.

14 101. Defendant maintained the Personal and Medical Information in a
15 reckless manner on network servers that were left vulnerable to cyberattacks.

16 102. Defendant knew of the importance of safeguarding Personal and
17 Medical Information and of the foreseeable consequences that would occur if
18 Plaintiff’s and Class members’ Personal and Medical Information was stolen,
19 including the significant costs that would be placed on Plaintiff and Class
20 members as a result of a breach of this magnitude.

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

27
28

³⁰*Id.*

1 104. Defendant disregarded the rights of Plaintiff and Class members by,
2 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take
3 adequate and reasonable measures to ensure that its network servers were
4 protected against unauthorized intrusions; (ii) failing to disclose that it did not
5 have adequately robust security protocols and training practices in place to
6 adequately safeguard Plaintiff’s and Class members’ Personal and Medical
7 Information; (iii) failing to take standard and reasonably available steps to prevent
8 the Data Breach; (iv) concealing the existence and extent of the Data Breach for
9 an unreasonable duration of time; and (v) failing to provide Plaintiff and Class
10 members prompt and accurate notice of the Data Breach.

11 **V. CLASS ACTION ALLEGATIONS**

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

14 106. Plaintiff brings all claims as class claims under Federal Rule of Civil
15 Procedure 23. Plaintiff asserts all claims on behalf of the proposed Nationwide
16 Class and Subclass, defined as follows:

17 **All persons residing in the United States whose personal and**
18 **medical information was compromised as a result of the**
19 **Data Breach that occurred in April 2021.**

20 **California Subclass: All persons residing in California**
21 **whose personal and medical information was compromised**
22 **as a result of the Data Breach that occurred in April 2021.**

23 107. Also, in the alternative, Plaintiff requests additional Subclasses as
24 necessary based on the types of Personal and Medical Information that were
25 compromised.

26 108. Excluded from the Nationwide Class and Subclass is Defendant, any
27 entity in which Defendant has a controlling interest, and Defendant’s officers,
28 directors, legal representatives, successors, subsidiaries, and assigns. Also

1 excluded from the Class is any judge, justice, or judicial officer presiding over this
2 matter and members of their immediate families and judicial staff.

3 109. Plaintiff reserves the right to amend the above definitions or to
4 propose alternative or additional Subclass in subsequent pleadings and motions for
5 class certification.

6 110. The proposed Nationwide Class and the Subclass (collectively
7 referred to herein as the “Class” unless otherwise specified) meet the requirements
8 of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

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

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

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

24 114. **Superiority:** A class action is superior to other available means of
25 fair and efficient adjudication of the claims of Plaintiff and the Class. The injury
26 suffered by each individual Class member is relatively small in comparison to the
27 burden and expense of individual prosecution of complex and expensive litigation.
28 It would be very difficult, if not impossible, for members of the Class individually

1 to effectively redress Defendant’s wrongdoing. Even if Class members could
2 afford such individual litigation, the court system could not. Individualized
3 litigation presents a potential for inconsistent or contradictory judgments.
4 Individualized litigation increases the delay and expense to all parties, and to the
5 court system, presented by the complex legal and factual issues of the case. By
6 contrast, the class action device presents far fewer management difficulties and
7 provides benefits of single adjudication, economy of scale, and comprehensive
8 supervision by a single court.

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

- 13 a. Whether Defendant engaged in the wrongful conduct alleged
14 herein;
- 15 b. Whether Defendant failed to adequately safeguard Plaintiff’s
16 and Class members’ Personal and Medical Information;
- 17 c. Whether Defendant’s systems, networks, and data security
18 practices used to protect Plaintiff’s and Class members’
19 Personal and Medical Information violated the FTC Act,
20 HIPAA, the CMIA, the UCL, and/or Defendant’s other duties
21 discussed herein;
- 22 d. Whether Defendant owed a duty to Plaintiff and the Class to
23 adequately protect their Personal and Medical Information, and
24 whether they breached this duty;
- 25 e. Whether Defendant knew or should have known that their
26 computer and network security systems were vulnerable to a
27 data breach;

- 1 f. Whether Defendant’s conduct, including their failure to act,
2 resulted in or was the proximate cause of the Data Breach;
- 3 g. Whether Defendant breached contractual duties to Plaintiff and
4 the Class to use reasonable care in protecting their Personal and
5 Medical Information;
- 6 h. Whether Defendant failed to adequately respond to the Data
7 Breach, including failing to investigate it diligently and notify
8 affected individuals in the most expedient time possible and
9 without unreasonable delay, and whether this caused damages
10 to Plaintiff and the Class;
- 11 i. Whether Defendant continue to breach duties to Plaintiff and the
12 Class;
- 13 j. Whether Plaintiff and the Class suffered injury as a proximate
14 result of Defendant’s negligent actions or failures to act;
- 15 k. Whether Plaintiff and the Class are entitled to recover damages,
16 equitable relief, and other relief;
- 17 l. Whether injunctive relief is appropriate and, if so, what
18 injunctive relief is necessary to redress the imminent and
19 currently ongoing harm faced by Plaintiff and members of the
20 Class and the general public;
- 21 m. Whether Defendant’s actions alleged herein constitute gross
22 negligence; and
- 23 n. Whether Plaintiff and Class members are entitled to punitive
24 damages.

25 **VI. CAUSES OF ACTION**

26 **A. COUNT I – NEGLIGENCE**

27 116. Plaintiff incorporates by reference all allegations of the preceding
28 paragraphs as though fully set forth herein.

1 117. Defendant solicited, gathered, and stored the Personal and Medical
2 Information of Plaintiff and the Class as part of the operation of its business.

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

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

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

16 121. Defendant was well aware of the fact that cyber criminals routinely
17 target large corporations through cyberattacks in an attempt to steal sensitive
18 personal and medical information.

19 122. Defendant owed Plaintiff and the Class members a common law duty
20 to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and
21 the Class when obtaining, storing, using, and managing personal information,
22 including taking action to reasonably safeguard such data.

23 123. Defendant's duty extended to protecting Plaintiff and the Class from
24 the risk of foreseeable criminal conduct of third parties, which has been
25 recognized in situations where the actor's own conduct or misconduct exposes
26 another to the risk or defeats protections put in place to guard against the risk, or
27 where the parties are in a special relationship. *See* Restatement (Second) of Torts
28

1 § 302B. Numerous courts and legislatures also have recognized the existence of a
2 specific duty to reasonably safeguard personal information.

3 124. Defendant had duties to protect and safeguard the Personal and
4 Medical Information of Plaintiff and the Class from being vulnerable to
5 cyberattacks by taking common-sense precautions when dealing with sensitive
6 Personal and Medical Information. Additional duties that Defendant owed
7 Plaintiff and the Class include:

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

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

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

- 1 a. Failing to exercise reasonable care in obtaining, retaining
- 2 securing, safeguarding, deleting, and protecting the Personal
- 3 and Medical Information in its possession;
- 4 b. Failing to protect the Personal and Medical Information in its
- 5 possession using reasonable and adequate security procedures
- 6 and systems;
- 7 c. Failing to adequately train its employees to not store Personal
- 8 and Medical Information longer than absolutely necessary;
- 9 d. Failing to consistently enforce security policies aimed at
- 10 protecting Plaintiff's and the Class's Personal and Medical
- 11 Information; and
- 12 e. Failing to implement processes to quickly detect data breaches,
- 13 security incidents, or intrusions;

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

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

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

25 130. As a result of the Data Breach, Plaintiff and Class members have
26 spent time, effort, and money to mitigate the actual and potential impact of the
27 Data Breach on their lives, including but not limited to, closely reviewing and
28 monitoring bank accounts, credit reports, and statements sent from providers and

1 their insurance companies and the payment for credit monitoring and identity theft
2 prevention services.

3 131. Defendant’s wrongful actions, inactions, and omissions constituted
4 (and continue to constitute) common law negligence.

5 132. The damages Plaintiff and the Class have suffered (as alleged above)
6 and will suffer were and are the direct and proximate result of Defendant’s grossly
7 negligent conduct.

8 133. In addition to its duties under common law, Defendant had additional
9 duties imposed by statute and regulations, including the duties under HIPAA, the
10 FTC Act, and the CMIA. The harms which occurred as a result of Defendant’s
11 failure to observe these duties, including the loss of privacy, significant risk of
12 identity theft, and Plaintiff’s overpayment for goods and services, are the types of
13 harm that these statutes and their regulations were intended to prevent.

14 134. Defendant violated these statutes when it engaged in the actions and
15 omissions alleged herein and Plaintiff’s injuries were a direct and proximate result
16 of Defendant’s violations of these statutes. Plaintiff therefore is entitled to the
17 evidentiary presumptions for negligence *per se* under Cal. Evid. Code § 669.

18 135. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty
19 to Plaintiff and the Class to provide fair and adequate computer systems and data
20 security to safeguard the Personal and Medical Information of Plaintiff and the
21 Class.

22 136. Defendant is an entity covered by HIPAA, 45 C.F.R. §160.102, and
23 as such is required to comply with HIPAA’s Privacy Rule and Security Rule.
24 HIPAA requires Defendant to “reasonably protect” confidential data from “any
25 intentional or unintentional use or disclosure” and to “have in place appropriate
26 administrative, technical, and physical safeguards to protect the privacy of
27 protected health information.” 45 C.F.R. § 164.530(c)(1). The confidential data at
28

1 issue in this case constitutes “protected health information” within the meaning of
2 HIPAA.

3 137. HIPAA further requires Defendant to disclose the unauthorized
4 access and theft of the protected health information of Plaintiff and the Class
5 “without unreasonable delay” so that Plaintiff and Class members could take
6 appropriate measures to mitigate damages, protect against adverse consequences,
7 and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404,
8 164.406, and 164.410.

9 138. The FTC Act prohibits “unfair practices in or affecting commerce,”
10 including, as interpreted and enforced by the FTC, the unfair act or practice by
11 businesses, such as Defendant, of failing to use reasonable measures to protect
12 Personal and Medical Information. The FTC publications and orders described
13 above also formed part of the basis of Defendant’s duty in this regard.

14 139. Defendant gathered and stored the Personal and Medical Information
15 of Plaintiff and the Class as part of its business of soliciting its services to its
16 patients, which solicitations and services affect commerce.

17 140. Defendant violated the FTC Act by failing to use reasonable
18 measures to protect the Personal and Medical Information of Plaintiff and the
19 Class and by not complying with applicable industry standards, as described
20 herein.

21 141. Defendant breached its duties to Plaintiff and the Class under the
22 FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer
23 systems and/or data security practices to safeguard Plaintiff’s and Class members’
24 Personal and Medical Information, and by failing to provide prompt notice
25 without reasonable delay.

26 142. Defendant’s failure to comply with applicable laws and regulations
27 constitutes negligence *per se*.

28

1 143. Plaintiff and the Class are within the class of persons that HIPAA and
2 the FTC Act were intended to protect.

3 144. The harm that occurred as a result of the Data Breach is the type of
4 harm the FTC Act and HIPAA were intended to guard against.

5 145. Defendant breached its duties to Plaintiff and the Class under these
6 laws by failing to provide fair, reasonable, or adequate computer systems and data
7 security practices to safeguard Plaintiff's and the Class's Personal and Medical
8 Information.

9 146. Defendant's violation of the FTC Act and HIPAA constitutes
10 negligence *per se*.

11 147. As a direct and proximate result of Defendant's negligence *per se*,
12 Plaintiff and the Class have suffered, and continue to suffer, damages arising from
13 the Data Breach, as alleged above.

14 148. The injury and harm that Plaintiff and Class members suffered (as
15 alleged above) was the direct and proximate result of Defendant's negligence *per*
16 *se*.

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

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

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

22 151. California established the right to privacy in Article 1, Section 1 of
23 the California Constitution.

24 152. The State of California recognizes the tort of Intrusion into Private
25 Affairs and adopts the formulation of that tort found in the Restatement (Second)
26 of Torts, which states, "One who intentionally intrudes, physically or otherwise,
27 upon the solitude or seclusion of another or his private affairs or concerns is
28 subject to liability to the other for invasion of his privacy if the intrusion would be

1 highly offensive to a reasonable person.” Restatement (Second) of Torts, § 652B
2 (1977).

3 153. Plaintiff and Class members had a legitimate and reasonable
4 expectation of privacy with respect to their Personal and Medical Information and
5 were accordingly entitled to the protection of this information against disclosure to
6 and acquisition by unauthorized third parties.

7 154. Defendant owed a duty to its patients, including Plaintiff and Class
8 members, to keep their Personal and Medical Information confidential.

9 155. The unauthorized access, acquisition, appropriation, disclosure,
10 encumbrance, exfiltration, release, theft, use, and/or viewing of Personal and
11 Medical Information, especially the type that is the subject of this action, is highly
12 offensive to a reasonable person.

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

22 157. The Data Breach constitutes an intentional interference with
23 Plaintiff’s and Class members’ interest in solitude or seclusion, either as to their
24 persons or as to their private affairs or concerns, of a kind that would be highly
25 offensive to a reasonable person.

26 158. Defendant acted with a knowing state of mind when it permitted the
27 Data Breach because it knew its information security practices were inadequate.
28

1 159. Acting with knowledge, Defendant had notice and knew that its
2 inadequate cybersecurity practices would cause injury to Plaintiff and Class
3 members.

4 160. As a proximate result of Defendant's acts and omissions, Plaintiff's
5 and Class members' Personal and Medical Information was accessed by, acquired
6 by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to,
7 stolen by, used by, and/ or reviewed by third parties without authorization, causing
8 Plaintiff and Class members to suffer damages.

9 161. Unless and until enjoined and restrained by order of this Court,
10 Defendant's wrongful conduct will continue to cause great and irreparable injury
11 to Plaintiff and Class members in that the Personal and Medical Information
12 maintained by Defendant can and will likely again be accessed by, acquired by,
13 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
14 by, used by, and/ or viewed by unauthorized persons.

15 162. Plaintiff and the Class have no adequate remedy at law for the
16 injuries in that a judgment for monetary damages will not end the invasion of
17 privacy for Plaintiff and Class members.

18 **C. COUNT III – BREACH OF IMPLIED CONTRACT**

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

21 164. When Plaintiff and the Class members provided their Personal and
22 Medical Information to Defendant when seeking medical services, they entered
23 into implied contracts in which Defendant agreed to comply with its statutory and
24 common law duties to protect Plaintiff's and Class members' Personal and
25 Medical Information.

26 165. Defendant required Plaintiff and Class members to provide Personal
27 and Medical Information in order to receive medical services.

28

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

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

8 168. Plaintiff and Class members would not have provided their Personal
9 and Medical Information to Defendant had they known that Defendant would not
10 safeguard their Personal and Medical Information, as promised.

11 169. Plaintiff and Class members fully performed their obligations under
12 the implied contracts with Defendant.

13 170. Defendant breached the implied contracts by failing to safeguard
14 Plaintiff's and Class members' Personal and Medical Information.

15 171. Defendant also breached the implied contracts when it engaged in
16 acts and/or omissions that are declared unfair trade practices by the FTC and state
17 statutes and regulations (including California's UCL), and when it failed to
18 comply with HIPAA, CMIA, and other state personal and medical privacy laws.
19 These acts and omissions included (i) representing that it would maintain adequate
20 data privacy and security practices and procedures to safeguard the Personal and
21 Medical Information from unauthorized disclosures, releases, data breaches, and
22 theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy
23 of the privacy and security protections for the Class's Personal and Medical
24 Information; and (iii) failing to disclose to the Class at the time they provided their
25 Personal and Medical Information that Defendant's data security system and
26 protocols failed to meet applicable legal and industry standards.

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

4 **D. COUNT IV – BREACH OF CONFIDENCE**

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

7 174. At all times during Plaintiff's and Class members' interactions with
8 Defendant, Defendant was fully aware of the confidential nature of the Personal
9 and Medical Information that Plaintiff and Class members provided to it.

10 175. As alleged herein and above, Defendant's relationship with Plaintiff
11 and the Class was governed by promises and expectations that Plaintiff and Class
12 members' Personal and Medical Information would be collected, stored, and
13 protected in confidence, and would not be accessed by, acquired by, appropriated
14 by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by,
15 and/or viewed by unauthorized third parties.

16 176. Plaintiff and Class members provided their respective Personal and
17 Medical Information to Defendant with the explicit and implicit understandings
18 that Defendant would protect and not permit the Personal and Medical
19 Information to be accessed by, acquired by, appropriated by, disclosed to,
20 encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by
21 unauthorized third parties.

22 177. Plaintiff and Class members also provided their Personal and Medical
23 Information to Defendant with the explicit and implicit understandings that
24 Defendant would take precautions to protect their Personal and Medical
25 Information from unauthorized access, acquisition, appropriation, disclosure,
26 encumbrance, exfiltration, release, theft, use, and/or viewing, such as following
27 basic principles of protecting their networks and data systems.
28

1 178. Defendant voluntarily received, in confidence, Plaintiff’s and Class
2 members’ Personal and Medical Information with the understanding that the
3 Personal and Medical Information would not be accessed by, acquired by,
4 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
5 by, used by, and/or viewed by the public or any unauthorized third parties.

6 179. Due to Defendant’s failure to prevent, detect, and avoid the Data
7 Breach from occurring by, inter alia, not following best information security
8 practices to secure Plaintiff’s and Class members’ Personal and Medical
9 Information, Plaintiff’s and Class members’ Personal and Medical Information
10 was accessed by, acquired by, appropriated by, disclosed to, encumbered by,
11 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third
12 parties beyond Plaintiff’s and Class members’ confidence, and without their
13 express permission.

14 180. As a direct and proximate cause of Defendant’s actions and/or
15 omissions, Plaintiff and Class members have suffered damages as alleged herein.

16 181. But for Defendant’s failure to maintain and protect Plaintiff’s and
17 Class members’ Personal and Medical Information in violation of the parties’
18 understanding of confidence, their Personal and Medical Information would not
19 have been accessed by, acquired by, appropriated by, disclosed to, encumbered by,
20 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third
21 parties. Defendant’s Data Breach was the direct and legal cause of the misuse of
22 Plaintiff’s and Class members’ Personal and Medical Information, as well as the
23 resulting damages.

24 182. The injury and harm Plaintiff and Class members suffered and will
25 continue to suffer was the reasonably foreseeable result of Defendant’s
26 unauthorized misuse of Plaintiff’s and Class members’ Personal and Medical
27 Information. Defendant knew its data systems and protocols for accepting and
28 securing Plaintiff’s and Class members’ Personal and Medical Information had

1 security and other vulnerabilities that placed Plaintiff's and Class members'
2 Personal and Medical Information in jeopardy.

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

22 **E. COUNT V – BREACH OF IMPLIED COVENANT OF GOOD**
23 **FAITH AND FAIR DEALING**

24 184. Plaintiff incorporates by reference all allegations of the preceding
25 paragraphs as though fully set forth herein.

26 185. As described above, Defendant made promises and representations to
27 Plaintiff and the Class that it would comply with HIPAA and other applicable
28 laws and industry best practices.

1 186. These promises and representations became a part of the contract
2 between Defendant and Plaintiff and the Class.

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

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

19 189. Plaintiff and Class members did all or substantially all significant
20 things that the contract required them to do.

21 190. Likewise, all conditions required for Defendant's performance were
22 met.

23 191. Defendant's acts and omissions unfairly interfered with Plaintiff's
24 and Class members' rights to receive the full benefit of their contracts.

25 192. Plaintiff and Class members have been harmed by Defendant's
26 breach of this implied covenant in the many ways described above, including
27 overpayment for services, imminent risk of certainly impending and devastating
28 identity theft that exists now that cyber criminals have their Personal and Medical

1 Information, and the attendant long-term time and expenses spent attempting to
2 mitigate and insure against these risks.

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

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

8 **F. COUNT VI – VIOLATIONS OF CALIFORNIA UNFAIR**
9 **COMPETITION LAW, Cal. Bus. & Prof. Code §17200, et seq.**

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

12 196. Plaintiff brings this Count against Defendant on behalf of the Class
13 or, alternatively, the California Subclass.

14 197. Defendant violated California’s Unfair Competition Law (“UCL”),
15 Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or
16 fraudulent business acts and practices and unfair, deceptive, untrue or misleading
17 advertising that constitute acts of “unfair competition” as defined in the UCL,
18 including, but not limited to, the following:

- 19 a. by representing and advertising that it would maintain adequate
20 data privacy and security practices and procedures to safeguard
21 Plaintiff’s and Class members’ Personal and Medical
22 Information from unauthorized disclosure, release, data breach,
23 and theft; representing and advertising that it did and would
24 comply with the requirement of relevant federal and state laws
25 pertaining to the privacy and security of the Class’s Personal and
26 Medical Information; and omitting, suppressing, and concealing
27 the material fact of the inadequacy of the privacy and security
28 protections for the Class’ Personal and Medical Information;

- b. by soliciting and collecting Class members' Personal and Medical Information with knowledge that the information would not be adequately protected, and by storing Plaintiff's and Class members' Personal and Medical Information in an unsecure electronic environment;
- c. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*; and
- d. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*

198. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, and the CMIA, Cal. Civ. Code § 56, *et seq.*

199. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above.

200. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class members' Personal and Medical Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

1 201. Plaintiff seeks relief under the UCL, including restitution to the Class
2 of money or property that the Defendant may have acquired by means of
3 Defendant’s deceptive, unlawful, and unfair business practices, declaratory relief,
4 attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and
5 injunctive or other equitable relief.

6 **G. COUNT VII – VIOLATIONS OF CALIFORNIA**
7 **CONFIDENTIALITY OF MEDICAL INFORMATION ACT,**
8 **Cal. Civ. Code § 56, et seq.**

9 202. Plaintiff incorporates by reference all allegations of the preceding
10 paragraphs as though fully set forth herein.

11 203. Plaintiff brings this Count against Defendant on behalf of the Class
12 or, alternatively, the California Subclass.

13 204. Defendant is a “provider of healthcare,” as defined in Cal. Civ. Code
14 § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code
15 §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

16 205. Defendant is licensed under California under California’s Business
17 and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et seq.* and
18 therefore qualifies as a “provider of healthcare” under the CMIA.

19 206. Plaintiff and the Class are “patients,” as defined in CMIA, Cal. Civ.
20 Code § 56.05(k) (“‘Patient’ means any natural person, whether or not still living,
21 who received healthcare services from a provider of healthcare and to whom
22 medical information pertains.”).

23 207. Defendant disclosed “medical information,” as defined in CMIA, Cal.
24 Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in
25 violation of Cal. Civ. Code § 56.10(a). The disclosure of information to
26 unauthorized individuals in the Data Breach resulted from the affirmative actions
27 and inactions of Defendant, including its failure to adequately implement
28 sufficient data security measures and protocols to protect Plaintiff’s and Class
members’ Personal and Medical Information, which allowed the hackers to see

1 and obtain Plaintiff's and the Class members' medical information.

2 208. Defendant's negligence resulted in the release of individually
3 identifiable medical information pertaining to Plaintiff and the Class to
4 unauthorized persons and the breach of the confidentiality of that information.
5 Defendant's negligent failure to maintain, preserve, store, abandon, destroy,
6 and/or dispose of Plaintiff's and Class members' medical information in a manner
7 that preserved the confidentiality of the information contained therein, in violation
8 of Cal. Civ. Code §§ 56.06 and 56.101(a).

9 209. Defendant's computer systems and protocols did not protect and
10 preserve the integrity of electronic medical information in violation of Cal. Civ.
11 Code § 56.101(b)(1)(A).

12 210. Plaintiff and the Class were injured and have suffered damages, as
13 described above, from Defendant's illegal disclosure and negligent release of their
14 medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and
15 therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages,
16 nominal statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief,
17 and attorney fees, expenses and costs.

18 **H. COUNT VIII – DECLARATORY RELIEF**

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

21 212. Plaintiff brings this Count under the federal Declaratory Judgment
22 Act, 28 U.S.C. §2201.

23 213. As previously alleged, Plaintiff and members of the Class were
24 parties to an implied contract with Defendant that required Defendant to provide
25 adequate security for the Personal and Medical Information it collected from them.

26 214. Defendant owed (and continues to owe) a duty of care to Plaintiff and
27 the members of the Class requiring Defendant to adequately secure Personal and
28 Medical Information.

1 215. Defendant still possess Plaintiff’s and Class members’ Personal and
2 Medical Information.

3 216. Since the Data Breach, Defendant has announced few if any changes
4 to its data security infrastructure, processes or procedures to fix the vulnerabilities
5 in its computer systems and/or security practices that permitted the Data Breach to
6 occur and go undetected for months.

7 217. Defendant has not satisfied its contractual obligations and legal duties
8 to Plaintiff and the Class. In fact, now that Defendant’s insufficient data security is
9 known to other ransomware attackers, the Personal and Medical Information in
10 Defendant’s possession is even more vulnerable to subsequent and continuous
11 cyberattacks.

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

19 219. There is no reason to believe that Defendant’s security measures are
20 any more adequate now than they were before the Data Breach to meet
21 Defendant’s contractual obligations and legal duties.

22 220. Plaintiff, therefore, seeks a declaration that Defendant’s existing
23 security measures do not comply with their contractual obligations and duties of
24 care to provide adequate security and that, to comply with their contractual
25 obligations and duties of care, Defendant must implement and maintain additional
26 security measures.

27 ///

28 ///

1 **VII. PRAYER FOR RELIEF**

2 WHEREFORE, Plaintiff and the Class pray for judgment against Defendant
3 as follows:

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

controls so that if one area of Defendant’s systems is compromised, hackers cannot gain access to other portions of Defendant’s systems;

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

vi. Ordering that Defendant conduct regular database scanning and securing checks; and

vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

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

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

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

VIII. DEMAND FOR JURY TRIAL

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

DATED: June 21, 2021

/s/ Bibianne U. Fell
Bibianne U. Fell, Esq.
Attorneys for Plaintiffs

EXHIBIT 1



Return mail will be processed by: IBC
PO Box 847, Holbrook, NY 11741



Kate Rasmuzzen

11

[Handwritten signature]

Corporate Compliance & Privacy Officer

June 1, 2021

Dear Kate Rasmuzzen:

Maintaining the confidentiality and security of our patients' information is something Scripps Health takes very seriously. Regrettably, we are writing to inform you of an incident involving some of that information.

On May 1, 2021, we identified unusual network activity. We immediately initiated our incident response protocols, which included isolating potentially impacted devices and shutting off select systems. We also began an investigation with the assistance of computer forensic firms. The investigation determined that an unauthorized person gained access to our network, deployed malware, and, on April 29, 2021, acquired copies of some of the documents on our system. On May 10, 2021, we discovered that some of those documents contained patient information. Upon conducting a review of those documents, we determined that one or more files may have reflected your name, address, date of birth, health insurance information, medical record number, patient account number, and/or clinical information, such as physician name, date(s) of service, and/or treatment information.

We have **no** indication that any of your information has been used to commit fraud. However, we recommend that you review the statements you receive from your healthcare providers and health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately. To help prevent something like this from happening again, we are continuing to implement enhancements to our information security, systems, and monitoring capabilities.

We deeply regret that this incident occurred and for any concern this may cause you. We value your trust and confidence in Scripps Health, and look forward to continuing to serve you.