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

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

**Pro Hac Vice* application to be submitted

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

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

Plaintiff,

v.

Scripps Health

Defendant.

Case No.: **'21CV1143 H DEB**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

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

I. INTRODUCTION

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

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

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

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

---

[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).

[2] *Id.*

[3] *See* https://www.scripps.org/patients-and-visitors/medical-records (last accessed June 18, 2021).

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

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

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

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

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

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

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

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

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

II. THE PARTIES

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

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

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

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

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

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

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

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

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

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

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

III. JURISDICTION AND VENUE

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

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

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

/ / /

/ / /

[5] *See* https://www.scripps.org/about-us (last accessed June 18, 2021).

IV. FACTUAL ALLEGATIONS

A. The California Attorney General Notice

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

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

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

27. Plaintiff's and Class members' Personal and Medical Information is "personal information" as defined by California Civ. Code § 1798.82(h).

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

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

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

/ / /

/ / /

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

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

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

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

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

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

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

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

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

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

B. The Data Breach and Defendant's Failed Response

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

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

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

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

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

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

/ / /

/ / /

46. Ransomware creators, such as the authors of Defendant's Data Breach, "are criminals without any ethics," so there is no guarantee they will do what they promise to do in exchange for any ransom money they receive.[6]

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

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

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

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

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

[6] https://enterprise.comodo.com/does-paying-ransomware-work.php (last accessed June 10, 2021).

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

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

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

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

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

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

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

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).

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[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.

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[12] *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/.

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

[14] *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/.

81. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[15]

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

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

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

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

---

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

[16] *Data Breaches Are Frequent*, *supra* note 11.

[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/.

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

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

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

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

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

---

[19] *Id.*

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

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

[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/.

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

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

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

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

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

---

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

[24] "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.

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

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

a. Trespass and damage their personal property, including Personal and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

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

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

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

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

h. The loss of use of and access to their credit, accounts, and/or funds.

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

/ / /

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

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

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

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

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

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

implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[30]

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

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

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

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

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

[30] *Id.*

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

V. CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Whether Defendant's systems, networks, and data security practices used to protect Plaintiff's and Class members' Personal and Medical Information violated the FTC Act, HIPAA, the CMIA, the UCL, and/or Defendant's other duties discussed herein;

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

e. Whether Defendant knew or should have known that their computer and network security systems were vulnerable to a data breach;

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

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

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

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

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

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

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

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

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

VI. CAUSES OF ACTION

A. COUNT I – NEGLIGENCE

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

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

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

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

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

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

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

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

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

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

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

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

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

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

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

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

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

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

c. Failing to adequately train its employees to not store Personal and Medical Information longer than absolutely necessary;

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

e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

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

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

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

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

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

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

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

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

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

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

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

issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

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

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

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

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

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

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

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

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

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

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

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

B. COUNT II – INVASION OF PRIVACY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. COUNT III – BREACH OF IMPLIED CONTRACT

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

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

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

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

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

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

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

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

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

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

D. COUNT IV – BREACH OF CONFIDENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class's Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security 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.

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

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

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

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

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

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

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

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

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

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

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

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

H. COUNT VIII – DECLARATORY RELIEF

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

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

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

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

215. Defendant still possess Plaintiff's and Class members' Personal and Medical Information.

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

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

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

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

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

/ / /

/ / /

VII. PRAYER FOR RELIEF

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

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

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

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

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

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

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access

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

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

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

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

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

e. A judgment in favor of 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

Scripps

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

Kate Rasmuzzen

11

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.