BETSY C. MANIFOLD (182450)
manifold@whafh.com
RACHELE R. BYRD (190634)
byrd@whafh.com
MARISA C. LIVESAY (223247)
livesay@whafh.com
BRITTANY N. DEJONG (258766)
dejong@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599

M. ANDERSON BERRY (262879)
aberry@justice4you.com
LESLIE GUILLON (222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

Attorneys for Plaintiff

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
06/07/2021 at 02:43:40 PM
Clerk of the Superior Court
By Maria Acevedo,Deputy Clerk

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

JOHNNY CORNING, on behalf of himself and all others similarly situated,

Plaintiff,

v.

SCRIPPS HEALTH,

Defendant.

Case No. 37-2021-00025007-CU-BT-CTL

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Johnny Corning ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Scripps Health ("Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for failure to adequately secure and safeguard electronically stored, personally identifiable information and protected health information ("PHI") that Defendant stored on its internal record systems for patients, staff and physicians,[1] including, without limitation, names, addresses, dates of birth, driver's license numbers, Social Security numbers, health insurance information, medical record numbers, patient account numbers, and/or clinical information such as physician names, date(s) of service, and/or treatment information (collectively, "personally identifiable information" or "PII").[2]

2. According to Defendant's website, Scripps Health is a $2.9 billion private, nonprofit, integrated health system in San Diego, California. Scripps treats 700,000 patients annually. The organization encompasses four hospitals on five campuses, as well as more than 3,000 affiliated physicians and 15,000 employees.[3]

3. Individuals entrust Defendant with an extensive amount of their PII and PHI. Defendant asserts that it understands the importance of protecting such information, that it "values

---

[1] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/, last visited June 6, 2021; https://www.sandiegouniontribune.com/news/health/story/2021-06-01/scripps-begins-notifying-more-than-147-000-people-of-ransomware-records-breach, last visited June 6, 2021.

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[3] https://www.scripps.org/about-us/who-we-are#:~:text=Scripps%20treats%20700%2C000%20patients%20annually,affiliated%20physicians%20and%2015%2C000%20employees, last visited June 6, 2021.

your privacy," and that it "take[s] care to protect and maintain the confidentiality of your information."[4]

4. On or before May 1, 2021, Defendant Scripps Health learned that an "unauthorized person" had gained access to its network, acquired electronic files, then deployed ransomware that took Scripps' systems offline on May 1, 2021; the electronic files stolen by the hackers contained the PII and PHI of Defendant's patients, staff and physicians, including that of Plaintiff and Class Members (the "Data Breach"). The data included, at least, Plaintiff's and Class Members' health information and Social Security numbers and/or driver's license numbers. Further, as a result of the attack, for weeks patients and staff were not able to gain access to the "MyScripps" portal which enabled patients to communicate with staff and doctors, access test results, request prescription refills, manage appointments, pay as a guest and view MyScripps video visit tutorials.[5]

5. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

6. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of their Social Security numbers, driver license numbers and/or specific, sensitive medical information.

7. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

8. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid storing and sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and

---

[4] https://www.scripps.org/privacy-policy, last visited June 6, 2021.

[5] https://myscripps.org/mychart/Authentication/Login?%5Fga=2%2E170351264%2E1236472328%2E1622584659%2D737447220%2E1622584659, last visited June 6, 2021.

state statutes.

9. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and, significantly, (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

11. Plaintiff Johnny Corning is a citizen of California residing in San Diego County, California.

12. Scripps Health is a $2.9 billion private, not-for-profit health system that serves the San Diego area through four acute-care hospitals. The health system treats 700,000 patients annually and also offers home health care and community outreach programs.[6]

[6] https://www.dnb.com/business-directory/company-profiles.scripps_health.81eaaaa141efad7365b7bf4d104a66d5.html, last visited June 6, 2021.

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

14. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

15. This Court has jurisdiction over the causes of action asserted herein pursuant to the California Constitution, article VI, section 10, because this case is a cause not given by statute to other trial courts and pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class Members pursuant to Cal. Code Civ. Proc. § 382. The amount in controversy exceeds the jurisdictional minimum of this Court. The amount in controversy as to the Plaintiff individually and each individual Class member does not exceed $75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. This action is not removable.

16. This Court has personal jurisdiction over Defendant because it is located within and regularly conducts business in California.

17. Venue is proper in this Court pursuant to Cal. Bus. & Prof. Code § 17203 and Cal. Code of Civ. Proc. §§ 390 and 395.5 because Defendant regularly conducts business in the State of California and in San Diego County; Defendant has obtained PII and PHI in the transaction of business in San Diego County, which has caused both Defendant's obligations and liability to arise in San Diego County; and Defendant's agent for service of process is located within San Diego County.

FACTUAL ALLEGATIONS

Background

18. Defendant Scripps operates a network system which contains electronic medical record applications, stores health information and stores personal financial information related to Defendant's patients, staff and physicians, including in the MyScripps portal. Upon information

and belief, the electronic files stored and/or shared by Defendant contained non-redacted and non-encrypted PII and PHI belonging to Plaintiff and Class Members. This sensitive and confidential PII, including, but not limited to, personal financial information, Social Security numbers, and/or driver's license numbers, is static and does not change, and can be used to commit myriad identity crimes. The PHI involved—personal health information—is also sensitive and confidential, and is protected, private medical treatment information that divulges underlying mental or physical diagnoses, as well as prescription, testing/laboratory results and other personal health information.

19. Plaintiff and Class Members relied on the sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

20. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

21. On or about May 12, 2021, *The San Diego Union-Tribune* reported that Scripps Health was attacked by hackers on May 1, 2021.[7]

22. The article questioned whether the hackers made off with "private medical or financial information when they attacked" or "did they just encrypt sever contents and demand a ransom?" Chris Van Gorder, Scripps' chief executive officer, stated that he could not share answers because the investigation was "ongoing." Patients were reported as saying they felt that "the lack of direct communication on the cybersecurity incident has been infuriating."[8]

23. On May 15, 2021, Scripps sent out an e-mail to their "Valued Scripps Patient[s]" addressing the "cyber security incident on May 1 that resulted in disruption to our IT systems at our hospitals and facilities."[9]

---

[7] https://www.sandiegouniontribune.com/news/health/story/2021-05-12/did-hackers-steal-records-before-ransomware-attack-sc, last visited June 6, 2021.

[8] *Id*.

[9] *See* Exhibit A.

24. On May 24, 2021, Scripps sent out a second e-mail to their "Valued Scripps Patient[s]" with an update to the cyber incident. The e-mail admits that the last few weeks "have been difficult for our community members," yet only acknowledges that the attack "involved ransomware."[10]

25. Finally, one month after the attack took place, Scripps provided a "statement" as reported by various online news sources which confirmed that an "unauthorized person" gained access to the network wherein "health information and personal financial information was acquired though other documents stored on our network."[11]

26. It was explained that the attackers ". . . lock the system down, and then they communicate with the victim/company, and they say, 'hey we will not unlock your system unless you pay us a ransom.'"[12]

27. Scripps also announced that it would be providing complimentary credit monitoring and identity protection "for the less than 2.5% of individuals whose Social Security number and/or driver's license number were involved." Scripps also stated that it was working to notify 147,267 people via mail to inform them to take steps to protect their information.[13]

28. On June 1, 2021, Scripps began to send two types of notices to Class Members notifying them of the Data Breach. The first notice stated, "Upon conducting a review of those documents, we determined that one or more files may have reflected your name, address, date of birth, Social Security number and/or driver's license number, 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."[14] The second notice stated, "Upon conducting a review of those documents, we determined that one or more files may have reflected

---

[10] *See* Exhibit B.

[11] https://www.cbs8.com/article/news/health/san-diegos-scripps-health-says-some-patient-info-acquired-during-ransomware-attack/509-26d07c96-4c42-4e22-8af9-8d579e0fbcb8, last visited June 6, 2021.

[12] *Id.*

[13] *Id.*

[14] https://oag.ca.gov/system/files/Scripps%20Health-%20Sample%20Notice.pdf, last visited June 6, 2021.

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."[15]

29. Defendant states in the notices that it is "continuing to implement enhancements to our information security, systems, and monitoring capabilities."[16] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with the states' Attorneys General or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

30. Plaintiff's and Class Members' non-encrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Because of this Data Breach, unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted information it was maintaining for Plaintiff and Class Members, causing their PII and PHI to be exposed.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

32. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and PHI.

33. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive, confidential PII and PHI.

34. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

35. Plaintiff and Class Members have taken reasonable steps to maintain the

[15] https://oag.ca.gov/system/files/Scripps-%20Letter%20Sample.pdf, last visited June 6, 2021.

[16] *Id.*

confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

36. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data that was no longer useful, especially outdated data.

37. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in light of the substantial increase in cyberattacks and/or data breaches in the healthcare and insurance industries preceding the date of the breach.

38. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would likely be targeted by cybercriminals.

39. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[17]

40. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare

[17] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware, last visited June 6, 2021.

organizations experienced cyberattacks in the past year.[18]

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

42. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

Defendant Scripps' Conduct Violates FTC Regulations

43. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

44. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Scripps Failed to Comply with HIPAA Standards of Conduct

45. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[21]

---

[18] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack, last visited June 6, 2021.

[19] 17 C.F.R. § 248.201(b)(9).

[20] 17 C.F.R. § 248.201(b)(8).

[21] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, *available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/, last visited June 6, 2021.

46. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling the type of PII and related data that Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

47. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendant to provide notice of the breach to each affected individual "*without unreasonable delay* and in no case later than 60 days following discovery of the breach."[22]

48. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits, in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronic

[22] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at:* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added), last visited June 6, 2021.

PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce, in violation of 45 C.F.R. § 164.306(a)(4);

h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. § 164.530(c).

Value of Personally Identifiable Information

49. It is well known that PII and PHI are invaluable commodities[23] and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[24] Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[25] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[26]

50. Consumers place a high value not only on their PII, but also on the privacy of that

---

[23] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[24] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf, last visited June 6, 2021.

[25] *Id*.

[26] *Id* at 15.

data. This is because identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

51. Defendant was well aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[27] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

52. There is a market for Plaintiff's and Class Members PII and PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.[28]

53. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

54. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

55. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing

---

[27] Federal Trade Commission, *What To Know About Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft, last visited June 6, 2021.

[28] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at:* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/, last visited June 6, 2021.

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."[29]

56. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[30]

57. The ramifications of Defendant's failure to keep its customers' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

58. Further, criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

59. Defendant knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's clients as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

---

[29] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at:* https://khn.org/news/rise-of-indentity-theft/, last visited June 6, 2021.

[30] FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at:* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf, last visited June 6, 2021.

Plaintiff Johnny Corning

60. Plaintiff received an outage notification on his Scripps Network portal stating that on May 1, 2021 Scripps Health experienced a cybersecurity incident that resulted in disruption to its IT systems at the Scripps hospitals and facilities.

61. On or around June 5, 2021, Plaintiff received a letter from Scripps via U.S. Mail dated June 1, 2021, informing him of the Data Breach.[31]

62. The June 1, 2021 letter notified Plaintiff that his 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 may have been exposed.

63. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone with Scripps attempting to restart his medical services/online medical classes, verifying the legitimacy of the Data Breach, monitoring his medical records for identity/informational theft, and self-monitoring his financial accounts. This time has been lost forever and cannot be recaptured.

64. Due to the IT outage, Plaintiff Corning was unable to gain access to his "MyScripps" portal account which contained the ability to communicate with doctors, access test results, request prescription refills, manage appointments, pay as a guest and view MyScripps video visit tutorials, which was necessary for his medical treatment.

65. Additionally, Plaintiff is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

66. Plaintiff stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

67. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that he entrusted to Defendant for the

[31] *See* Exhibit C.

purpose of obtaining medical evaluation and treatment from Scripps, which was compromised in and as a result of the Data Breach.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, as well as anxiety over losing access to the "MyScripps" portal.

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

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

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this action on his own behalf and as a class action, pursuant to California Code of Civil Procedure section 382, on behalf of the following class:

> All California residents whose PII and/or PHI was compromised in the Data Breach beginning on or about May 1, 2021 as disclosed by Defendant Scripps on or about May 15, 2021 (the "Class").

Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

72. This action is properly maintainable as a class action.

73. The Class is so numerous that joinder of all members would be impracticable.

74. Plaintiff is committed to prosecuting the action and have retained competent counsel experienced in litigation of this nature. Plaintiff's claims are typical of the claims of the other members of the Class, and Plaintiff has the same interests as the other members of the Class. Plaintiff is an adequate representative of the Class.

75. Questions of law and fact common to the members of the Class predominate over any questions affecting any individual member, and a class action is superior to all other available

methods for the fair and efficient adjudication of the controversy.

76. The common questions of law and fact include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the

Data Breach.

77. Plaintiff is a member of the Class he seeks to represent and his claims and injuries are typical of the claims and injuries of the other Class Members.

78. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. Plaintiff and his counsel will fairly and adequately protect the interests of Class Members.

79. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

80. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the Class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

81. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

82. Plaintiff and the Class provided and entrusted Defendant with certain PII and PHI, including but not limited to personal health information, personal financial information, Social

Security numbers and driver's license numbers.

83. Plaintiff and the Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

84. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Class could and would suffer if the PII and PHI were wrongfully disclosed.

85. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

86. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

87. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations.

88. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Class.

89. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class, which is recognized by laws and regulations including but not limited to HIPAA, as well as the common law. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

90. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably safeguard" 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).

91. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

92. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

93. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

94. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and/or storing the PII and PHI of Plaintiff and the Class on its computer systems.

95. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

96. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

97. Plaintiff and the Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

98. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

99. Defendant had and continues to have a duty to adequately disclose that the PII and

PHI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

100. Defendant has a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Class.

101. Defendant admitted that the PII and PHI of Plaintiff and the Class were "acquired" by an "unauthorized person," who then deployed ransomware that took Defendant's systems offline on May 1, 2021.

102. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Class during the time the PII and PHI were within Defendant's possession or control.

103. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach, including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2 of the NIST Cybersecurity Framework Version 1.1.

104. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Class in the face of increased risk of theft.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

106. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI that was no longer required to retain pursuant to regulations.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII and PHI of Plaintiff and the Class would not have been compromised.

109. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII and PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

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

111. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

113. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

114. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

115. Defendant's misconduct also included its decision not to comply with HIPAA for the reporting, safekeeping and encrypted authorized disclosure of the PHI of Plaintiff and Class Members.

116. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

117. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

118. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

119. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI and PHI I; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

120. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

121. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

122. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

123. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII and PHI.

124. Defendant required Plaintiff and the Class to provide and entrust their PII and PHI, including full names, birthdates, Social Security numbers, driver's license numbers, prescription information, health insurance information, and/or other information, as a condition of obtaining medical care and/or as a condition of employment.

125. Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

126. As a condition of being customers and/or employees of Defendant, Plaintiff and the Class provided and entrusted their PII and PHI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

127. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the protection of their PII and PHI.

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

129. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their PII and PHI by failing to provide timely and accurate notice to them that their PII and PHI was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

131. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

132. Plaintiff and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

133. Defendant owed a duty to Plaintiff and the Class to keep their PII and PHI confidential.

134. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII and PHI of Plaintiff and the Class.

135. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and the Class by way of Defendant's failure to protect the PII and PHI.

136. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Class is highly offensive to a reasonable person.

137. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII and PHI to Defendant as part of Plaintiff's and the Class' relationships with Defendant, but privately and with the intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

138. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class' 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.

139. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

140. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

141. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

142. 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 the Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. 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 the Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Class)

143. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

144. At all times during Plaintiff's and the Class' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class' PII and PHI that Plaintiff and the Class provided to Defendant.

145. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

146. Plaintiff and the Class provided their PII to Defendant with the explicit and implicit understanding that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

147. Plaintiff and the Class also provided their PII and PHI to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

148. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the Class with the understanding that their PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

149. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII and PHI of Plaintiff and the Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class' confidence, and without their express permission.

150. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

151. But for Defendant's disclosure of Plaintiff's and the Class' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct

and legal cause of the theft of Plaintiff's and the Class' PII and PHI as well as the resulting damages.

152. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class' PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class' PII and PHI.

153. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of their PII and PHI as a result of the Data Breach for the remainder of Plaintiff's and the Class Members' lives.

As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of Plaintiff and the Class)

154. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

155. Defendant has violated Cal. Bus. and 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 Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

156. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PII and PHI of Plaintiff and the Class with knowledge that the information would not be adequately protected; and by storing the PII and PHI of Plaintiff and the Class in an unsecure environment in violation of HIPAA and the rules and regulations promulgated thereunder, including 42 U.S.C. § 1301, *et seq*., 45 C.F.R. §§ 164.400-414, and 45 C.F.R. § 164.306, *et seq*. (as alleged *supra*.); and in violation of the Federal Trade Commission Act, 15 U.S.C. § 45 and 17 C.F.R. § 248.201, which require Defendant to employ reasonable methods of safeguarding the PII and PHI of Plaintiff and the Class.

157. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and the Class' legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

158. Defendant knew or should have known that its data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the Class and that the risk of a data breach or theft was highly likely, especially given its inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

159. Plaintiff and the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and the Class of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

COUNT VI
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of Plaintiff and the Class)

160. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

161. Defendant engaged in unfair acts and practices with respect to the services it provides by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PII and PHI of Plaintiff and the Class with knowledge that the information would not be adequately protected; and by storing the PII and PHI of Plaintiff and the Class in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Class. They were likely to deceive the public into believing their PII and PHI was securely stored, when it was not. The harm these practices caused to Plaintiff and the Class outweighed their utility, if any.

162. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the PII and PHI of Plaintiff and the Class from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Class. They were likely to deceive the public into believing their PII and PHI were securely stored when they were not. The harm these practices caused to Plaintiff and the Class outweighed their utility, if any.

163. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and the Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and the Class' legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

164. Defendant knew or should have known that its data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the Class and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class.

165. Plaintiff and the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the Class of money or property that the Defendant may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

COUNT VII
Violation of the Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq*.
(On Behalf of Plaintiff and the Class)

166. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

167. At all relevant times, Defendant was healthcare provider for the purposes of this cause of action because it had the "purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code § 56.06(a).

168. Defendant maintains medical information as defined by Cal. Civil Code § 56.05(j).

169. Plaintiff and Class Members are patients of Defendant for the purposes of this cause of action, as defined in Cal. Civil Code § 56.05(k).

170. Plaintiff and Class Members provided their PII and PHI to Defendant.

171. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff's and Class Members' personal medical information.

172. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

173. As a result of the Data Breach, Defendant misused, disclosed, and/or allowed third parties to access and view Plaintiff's and Class Members' personal medical information without their written authorization compliant with the provisions of Cal. Civil Code § 56, *et seq*.

174. As a further result of the Data Breach, the confidential nature of Plaintiff's and Class Members' medical information was breached as a result of Defendant's negligence. Specifically, Defendant knowingly and affirmatively acted in a manner that actually allowed unauthorized parties to access, view, and use Plaintiff's and Class Members' PHI.

175. Defendant's misuse and/or disclosure of Plaintiff's and Class Members' medical information constitutes a violation of Cal. Civil Code §§ 56.10, 56.11, and 56.26.

176. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' personal medical information was disclosed without written authorization.

177. By disclosing Plaintiff's and Class Members' PII and PHI without their written authorization, Defendant violated California Civil Code § 56, *et seq*., and its legal duties to protect the confidentiality of such information.

178. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

179. As a direct and proximate result of Defendant's wrongful actions, inaction, and omissions of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

180. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under Cal. Civil Code §§ 56.35, 56.36.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. An Order certifying the Class and the Class, and appointing Plaintiff and his Counsel to represent each such Class;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members;

C. Injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to

the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent 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;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. An award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. Prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: June 7, 2021

Respectfully Submitted,

RACHELE R. BYRD

BETSY C. MANIFOLD (182450)
RACHELE R. BYRD (190634)
MARISA C. LIVESAY (223247)
BRITTANY N. DEJONG (258766)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
manifold@whafh.com
byrd@whafh.com
livesay@whafh.com
dejong@whafh.com

M. ANDERSON BERRY (262879)
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiff

27418/SCRIPPS

EXHIBIT A

[redacted]

[redacted]

[redacted]

-------- Original message --------
From: Scripps Health <noreply@scrippshealth-email.org>
Date: 5/15/21 1:20 PM (GMT-08:00)
To: [redacted]
Subject: Important Update from Scripps Health

Scripps

Dear Valued Scripps Patient,

As you may have heard, Scripps Health experienced a cyber security incident on May 1 that resulted in disruption to our IT systems at our hospitals and facilities. Now, as always, providing you with the care you need is our number one priority. We remain open and here for you. We are working around the clock to restore our systems and have in place back up processes so we can continue to serve you, so please don't hesitate to come in for needed care. As we work through this issue, we wanted to keep you informed by sharing with you answers to some of the questions we are being asked in the hope they may prove helpful to you. Please know if you need more assistance, you can reach out to 1-800-SCRIPPS (1-800-727-4777). We appreciate your patience and understanding.

BACKGROUND

What caused the Scripps network outage?

In response to the cyber security incident on May 1, our team immediately took steps to contain the malware by taking a significant portion of our network offline. We also immediately engaged outside consultants and experts to assist us in our investigation and other experts to help us restore our systems and get back online as soon as possible.

When will systems be restored?

Providing the quality and continuity of care that our patients expect from us is our priority. We are continuing to work diligently to restore our systems as quickly and as safely as possible. This process is ongoing and will take time to complete. Unfortunately, we are not able to provide a specific timetable at this time.

ACCESS TO CARE

Can I currently access care at Scripps?

Yes, our hospitals, Emergency Departments, Urgent Care Centers, Scripps HealthExpress, Scripps Clinic and Scripps Coastal sites and affiliated practices are open and seeing patients.

How can I confirm an existing appointment or schedule a new appointment?

We recommend contacting your provider directly to check on an existing appointment. For questions or assistance, please call 1-800-SCRIPPS (800-727-4777). For new appointments, please call your provider. Scripps is currently scheduling patients for up to one week out. If you need an appointment beyond that time frame, your doctor’s office will collect your contact information and will follow up once our systems are back online.

Are elective surgeries and procedures being postponed?
Physician and staff leadership at each site are reviewing scheduled surgeries, infusions, imaging, lab and all other patient care services regularly. If certain services and appointments need to be rescheduled, we are reaching out to patients directly when possible.

What should I expect at my in-person appointment?
Our team prepares for this type of situation and has back-up workflows and paper processes in place to make sure patients are getting the care and support they need. When patients arrive for a scheduled appointment, clinical staff will meet them at each entrance to discuss options for their care. The patient care teams have view-access to certain patient history and records at this time.

Are virtual appointments still available?
Yes, virtual visits are still taking place. Your doctor's office should reach out to you with instructions on how to connect with your doctor prior to your virtual visit. You can also reach out to your doctor's office to confirm your visit if you don't hear from them within an hour of your visit.

Are Urgent Care wait times impacted?
We are actively monitoring patient wait times and turnaround times at our Scripps Urgent Care locations. As of today, they continue to be within normal range with no interruption of care.

ANCILLARY SERVICES AND SUPPORT

What do I do if I need imaging or radiology services?
We are working closely with our network partner, Imaging Healthcare Specialists (IHS) to support imaging appointments for patients for any

cancelled exams, or with any new imaging needs. IHS is owned by Scripps Health, and was unaffected by the network outage. IHS has multiple imaging centers and outpatient procedure centers throughout San Diego.

Can I still get a lab test?

Scripps has partnered with Quest Diagnostics and Labcorp to help provide laboratory services while we are working to restore our systems. If you need routine blood work or lab tests, please contact your provider for further instructions on where to go or contact the Scripps Lab Service Center at 858-554-9552.

How do I get prescription refills?

If you generally fill at a Scripps retail pharmacy, please call the pharmacy to assist with your refill. If you use a non-Scripps retail pharmacy, we recommend checking back with them to see if you can now access your prescription refill or get an emergency supply.

What if I need a COVID-19 test?

Scripps continues to support COVID-19 testing for symptomatic patients. Patients will receive a phone call with their positive or negative result.

BILLING

Will I be charged a late fee if my bill is not paid on time?

Accounts will not default, be considered late, or sent to collections during this network outage. There will also be a grace period of 14 days after our systems go live to make payments to your account and be considered on time.

PATIENT DATA

Has my personal data been compromised?

The investigation into the scope of the incident, including whether data was potentially affected, remains ongoing. Depending on the investigation's findings, we will be sure to provide notifications to affected individuals in accordance with all applicable laws.

Scripps has served this community for 100 years. We will come through this. We are here for you, now. And we will be here for generations of patients to come. Thank you again for your patience and understanding during this challenging time. And please, reach out to us at 1-800-SCRIPPS if you need further assistance.

Anil N. Keswani, M.D.
Chief Medical Officer,
Ambulatory and Accountable Care

Ghazala Sharieff, M.D., MBA
Chief Medical Officer,
Acute Care, Clinical Excellence and Experience

This email was sent by:
Scripps Health
10010 Campus Point Drive,
San Diego, CA, 92121
Update Preferences
Unsubscr be
Privacy Policy
© 2018 Scripps Health

EXHIBIT B

[redacted]

[redacted]

-------- Original message --------
From: Scripps Health <reply@scrippshealth-email.org>
Date: 5/24/21 2:32 PM (GMT-08:00)
To: [redacted]
Subject: Important information from Scripps Health.

Scripps

Dear Valued Scripps Patient,

I want to provide an update for you about Scripps' continued response to our recent cyber incident. We know the last few weeks have been difficult for our community members, and at times it may have seemed like we weren't communicating enough. We care deeply about our relationship with you and all of our patients, and I am sorry this has caused frustration.

In our current situation, openly sharing the details of the work we have been doing puts Scripps at an increased risk of coming under further attack, and of not being able to restore our systems safely and as quickly as possible for you. This is not hypothetical. Other attackers are already using what is being reported in the media to send scam communications to our organization. I know that, for some of you, the reasons why we haven't provided more frequent updates may not matter. But it was important for me to share and assure you that our patients', employees', and physicians' safety and security

are our constant guides.

That being said, we are now at a point where we can share some additional updates. We are continuing to investigate the incident, which I can confirm involved ransomware. We reported this to federal law enforcement, and continue to support their investigation as well. Our IT teams and outside consultants are literally working around the clock to restore our systems. Rest assured, we have thorough backups and are using them to help our restoration efforts. Even so, there is no “easy button.”

We continue to make progress. When you come in for care, your medical history is again at our fingertips electronically, and we’ve increased capacity at our internal call center to help answer patients’ questions. In addition, we anticipate our electronic health record will be back online the latter part of this week, including your ability to log into your MyScripps account to see your health care information. While this progress is meaningful, there is work left to be done. We look forward to building on these efforts and restoring the remaining Scripps systems as soon as possible.

In the meantime, as always, providing you with exceptional health care is our number one priority, so please don’t hesitate to come in for needed care.

We know that this incident has been a hardship for our patients, our employees, and our physicians, and we are truly sorry.

Thank you again for your patience and understanding during this challenging time. We are committed to continuing to serve you and our community, and will continue to provide you with updates.

Thank you,
Chris Van Gorder
President and CEO
Scripps Health

This email was sent by:
Scripps Health
10010 Campus Point Drive,
San Diego, CA, 92121
Update Preferences
Unsubscr be
Privacy Policy
© 2021 Scripps Health

EXHIBIT C

Scripps

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

40050090000056927
000 0000274 00000000 0001 0001 00274 INS: 0 0

JOHNNY CORNING
[redacted]
SAN DIEGO CA [redacted]

June 1, 2021

Dear Johnny Corning:

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.

If you have any questions, please call the dedicated call center established for this matter at 1-855-535-1822, Monday through Friday, between 6:00 a.m. and 6:00 p.m. Pacific Time.

Sincerely,

Taunya Juliano
Corporate Compliance & Privacy Officer