James Robert Noblin (State Bar No. 114442)
GREEN & NOBLIN, P.C.
4500 East Pacific Coast Highway, Fourth Floor
Long Beach, CA 90804
Telephone: (562) 391-2487
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

Robert S. Green (State Bar No. 136183)
GREEN & NOBLIN, P.C.
2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

Counsel for Plaintiffs

[Additional Counsel Appear on Signature Page]

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

JUAN MALDONADO, and all similarly situated individuals,

Plaintiffs,

v.

SOLARA MEDICAL SUPPLIES, LLC.,

Defendant.

Case No.: '19CV2284 H KSC

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Juan Maldonado, individually ("Plaintiff') and on behalf of all others similarly situated, brings this action against Defendant Solara Medical Supplies, LLC, based on personal knowledge and on information and belief from the investigation of counsel, and alleges and states as follows:

I. INTRODUCTION

1. Between April 2, 2019 and June 20, 2019, hackers infiltrated and accessed the inadequately protected computer systems of Defendant Solara Medical Supplies, LLC ("Solara"). The hackers gained access to Solara's computer systems with the intent to steal the protected personal information and protected health information of the millions of individuals whose information was stored on Defendant's computer systems (the "Data Breach"). And the hackers were successful with respect to potentially thousands of these individuals ("Breach Victims").

2. The personal information taken by the hackers includes: names, addresses, dates of birth, Social Security numbers, Employee Identification Numbers, and perhaps even more damaging to the Breach Victims, their personal and confidential: medical information, health insurance information, passwords, pins, or account login information, billing and claims information, and Medicare and Medicaid IDs, as well as financial information, credit and debit card information, driver's licenses and state identification cards, passport information (collectively, "Personal and Medical Information").

3. In short, thanks to Defendant's failure to protect the Breach Victims' Personal and Medical Information, cyber criminals were able to steal everything they could possibly need to commit nearly every conceivable form of identity theft and wreak havoc on the financial and personal lives of potentially millions of individuals.

4. Defendant's conduct-failing to implement adequate and reasonable measures to ensure their computer systems were protected, failing to take adequate steps to prevent and stop the breach, failing to timely detect the breach, failing to disclose the material facts that they did not have adequate computer systems and security practices to safeguard the Personal and Medical Information, failing to honor their repeated promises and representations to protect the Breach Victims' Personal and Medical Information, and failing to provide timely and adequate notice of the Data Breach-caused substantial harm and injuries to Breach Victims across the United States.

5. As a result of the Data Breach, Breach Victims have been suffered damages. For example, Breach Victims have had fraudulent charges on various financial accounts. They have spent many hours filing police reports and monitoring credit reports and credit and bank accounts to combat identity theft. Many are now paying monthly or annual fees for identity theft and credit monitoring services. Now that their Personal and Medical Information has been released into the criminal cyber domains, Breach Victims must spend their time being extra vigilant due to Defendant's failures to try to prevent being victimized for the rest of their lives.

6. Plaintiff brings this class action lawsuit on behalf of a nationwide class and state subclasses to hold Defendant responsible for its negligent-indeed, reckless-failure to use reasonable, current cybersecurity measures to protect class members' Personal and Medical Information.

7. Because Defendant presented such a soft target to cybercriminals, Plaintiff and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and class members must now and in the future, take their time to more closely monitor their financial accounts to guard against identity theft.

8. Plaintiff and class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

9. On behalf of himself and all Breach Victims, Plaintiff seeks actual damages, statutory damages, and punitive damages, with attorney fees, costs, and expenses under the California Consumer Privacy Act, Cal. Civ. Code § 1798.80, California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code § 56, other state personal and medical privacy laws, consumer protection and unfair and deceptive practices acts, negligence, negligence per se, and breach of implied contract. Plaintiff also seeks injunctive relief, including significant improvements to Defendant's data security systems, future annual audits, and long-term credit monitoring services funded by Defendant, and other remedies as the Court sees fit.

II. THE PARTIES

10. Plaintiff Juan Maldonado is a citizen and a resident of Delaware County, Pennsylvania.

11. Defendant Solara Medical Supplies, LLC is a California limited liability company with its principal place of business in Chula Vista, California, in San Diego County.

III. JURISDICTION AND VENUE

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

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 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 many members of the class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class members reside in this District.

15. Venue as to Defendant is proper in this judicial district under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL ALLEGATIONS

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

Defendant

17. Defendant is the largest direct-to-patient supplier of advanced diabetic devices, including continuous glucose monitors, insulin pumps and other supplies for patients with diabetes. It also supplies medical devises for the treatment of other conditions.

18. As part of Defendant's business, Defendant collects substantial amounts of Personal and Medical Information. The information Defendant collects qualifies as "Personal information" under the California Customer Records Act, Cal. Civ. Code § 1798.80, and other state data breach and information privacy acts, including the Pennsylvania Breach of Personal Information Notification Act, 73 Pa. Stat. § 2302. The medical information that Defendant collects qualifies as "Medical information" under the federal Health Information Portability and Accountability Act (HIPAA), the California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code § 56, *et seq.*, and other state medical record protection acts.

Plaintiff

19. Plaintiff used Solara medical devices to manage a health condition.

20. To receive the medical devices from Defendant, Plaintiff was required to provide Defendant with his Personal and Medical Information.

21. On or about November 20, 2019, Plaintiff received a letter from Solara, dated November 11, 2019, informing him that his "name, date of birth, medical information, and health insurance information" was compromised in the Data Breach. *See* Exhibit 1 (*Letter from Martin Hoffman to Juan Maldonado*, dated November 11, 2019).

22. Because of the Data Breach, Plaintiff's Personal and Medical Information is now in the hands of cyber criminals. He, and all Breach Victims like him, are now imminently at risk of crippling identity theft and fraud.

23. Plaintiff has not been the victim of any previous data breach to his knowledge.

24. Plaintiff trusted Solara with his Personal and Medical Information, and Solara violated that trust. Due to the nature of the medical devices Solara provides, Plaintiff may nevertheless have to continue using Solara devices. Plaintiff is therefore extremely concerned that there be Court-ordered improvements to Solara's privacy and cyber security practices to prevent this type of breach and failure by Defendant from ever happening again.

A. The Data Breach

25. On or around November 13, 2019, Solara issued a press release (the "Notice") providing, for the first time, a public notice of "an incident that may

affect the security of some information relating to certain individuals associate with Solara including current and former patients and employees."[1]

26. In the Notice, Solara notified consumers that on June 28, 2019—over four and a half months earlier—it had "determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019." It went on to say that within five days of this discovery, Solara confirmed with assistance from third-party forensic experts that Personal and Medical Information within those email accounts "may have been accessed or acquired by an unknown actor at the time of the incident."[2]

27. Yet, despite knowing many patients were in danger, Defendant did nothing to warn Breach Victims until over four months later. During this time, the cyber criminals had free reign to defraud their unsuspecting victims. Solara apparently chose to complete its internal investigation and develop its excuses and speaking points before giving class members the information they needed to protect themselves against fraud and identity theft.

28. After its "comprehensive manual and programmatic review," Defendant determined that:

> The personal information present in the accounts at the time of the incident varied by individual but may have included first and last names and one or more of the following data elements: name, address, date of birth, Social Security number, Employee Identification Number, medical information, health insurance information, financial information, credit / debit card information, driver's license / state ID, passport information, password / PIN or account login information, billing / claims information, and Medicare ID / Medicaid ID.[3]

This was a staggering coup for the cyber criminals and a stunningly bad showing for Defendant.

[1] "Solara Medical Supplies Provides Notice of a Data Breach," PR Newswire, Nov. 13, 2019, https://www.prenewswire.com/news-releases/solara-medical-supplies-provides-notice-of-a-data-breach-300957962.html.
[2] *Id*
[3] *Id*

29. In spite of the severity of the Data Breach, Defendant has done very little to protect Breach Victims. In the Notice, Solara states that it is notifying Breach Victims "so that they may take further steps to best protect their information, *should they feel it is appropriate to do so.*"[4] In effect, shirking its responsibility for the harm it has caused and putting it all on the Breach Victims.

30. Defendant Solara failed to adequately safeguard class members' Personal and Medical Information, allowing the cyber criminals to access this wealth of priceless information for nearly two full months, and then use it for another four months before Solara warned the criminals' victims, the Breach Victims, to be on the lookout.

31. Defendant Solara failed to spend sufficient resources on monitoring external incoming emails and training its employees to identify email-born threats and defend against them.

32. Defendant had obligations created by HIPPA, the California Medical Information Act (CMIA), reasonable industry standards, its own contracts with its patients and employees, common law, and its representations to Class Members, to keep their Personal and Medical Information confidential and to protect the information from unauthorized access.

33. Plaintiff and class members provided their Personal and Medical Information to Solara with the reasonable expectation and mutual understanding that Solara would comply with its obligations to keep such information confidential and secure from unauthorized access.

34. Indeed, as discussed below, Solara promised patients that it would do just that.

[4] *Id.* (emphasis added).

B. Defendant Promised to Protect Personal and Medical Information

35. Solara provides all patients, including Plaintiff, its Notice of Privacy Practices. In fact, Solara is required to do so by federal and state law. Solara's Notice of Privacy Practices states, as relevant:

> Solara Medical Supplies, Inc. . . . is committed to protecting your privacy and understands the importance of safeguarding your personal health information. We are required by federal law to maintain the privacy of health information that identifies you or that could be used to identify you . . . .[5]

36. Likewise, Solara provides every patient a "Patient Bill of Rights" that assures the patients of their right to the confidentiality of all their records provided to, generated by, or retained by Solara:

> The Client Bill of Rights is designed to recognize, promote, and protect, an individual's right to be treated with dignity and respect within the health care system. . . . As our client you have the right to . . . Confidentiality of your records and Solara Medical Supplies, LLC policy for accessing and disclosure of records.[6]

37. While Solara claims it is committed to protecting patients' privacy, recent events prove otherwise.

38. If Solara truly understands the importance of safeguarding patients' Personal and Medical Information, it should compensate class members for their losses, provide long-term protection for the Class, and agree to Court-ordered and enforceable changes to its cybersecurity policies and procedures and adopt regular and intensive training to ensure that something like this never happens again.

39. Defendant's data security obligations were particularly important given the known substantial increase in data breaches in the healthcare industry, including the recent massive data breach involving LabCorps, Quest Diagnostics,

[5] Solara Medical Supplies, "Notice of Privacy Practices," Effective Date: March 1, 2010, https://www.solara.com/privacy-policy (last accessed November 26, 2019).
[6] Solara Medical Supplies, "Patient Bill of Rights," https://www.solara.com/patient-bill-of-rights (last accessed November 26, 2019).

and American Medical Collections Agency. And given the wide publicity given to these data breaches, there is no excuse for Solara's failure to adequately protect class members' Personal and Medical Information.

40. That information, is now in the hands of cyber criminals who will use it if given the chance. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to consumers.

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

41. Defendant is a "business associate" covered by HIPPA. As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part 160 and Part 164.

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

43. HIPAA's Security 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 health or transferred in electronic form.

44. 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.

45. "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.

46. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the . . . 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 . . . .

d. Ensure compliance . . . by its workforce.

47. 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).

48. HIPAA also requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

49. Defendant is also prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission has found 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 Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

50. As described before, Defendant is also required by various state laws and regulations to protect Plaintiff's and Class Members' Personal and Medical Information.

51. In addition to their obligations under federal and state laws, Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant 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 Breach Victims to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal and Medical Information of the Breach Victims.

52. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to design, maintain, and test its computer systems and email system to ensure that the Personal and Medical Information in Defendant's possession was adequately secured and protected.

53. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal and Medical Information.

54. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

55. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

56. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

57. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant 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.

58. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

59. Defendant owed a duty of care to Breach Victims because they were foreseeable and probable victims of any inadequate data security practices.

D. Defendant Was on Notice of Cyber Attack Threats and the Inadequacy of Its Data Security

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

61. Defendant was on notice that the FBI has 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)."[7]

62. Defendant was on notice that the federal government has been concerned about healthcare company data encryption. Defendant knew it kept protected health information in its email accounts and yet did not encrypt its email accounts.

63. 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."[8]

E. A Data Breach like Solara's Results in Debilitating Losses to Consumers

64. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[9] Cyber criminals can leverage Plaintiff's and class members' Personal and Medical Information that was stolen in the Data Breach to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain medical services and government benefits, using Breach Victims' Personal Information to file fraudulent tax returns, using Breach Victims' health insurance information to rack up massive medical debts in their names, using Breach Victims' health information to target other

[7] 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.

[8] [8]"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.

[9] "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").

phishing and hacking intrusions based on their individual health needs, using Breach Victims' information to obtain government benefits, filing fraudulent tax returns using Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

65. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

66. This was a financially motivated data breach, as the only reason the cyber criminals stole Plaintiff's and the Class Members' Personal and Medical Information from Solara was to engage in the kinds of criminal activity described in paragraph 63, which will result, and has already begun to, in devastating financial and personal losses to Breach Victims.

67. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they ***will*** use it.[10]

68. 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.[11]

[10] Ari Lazarus, "How fast will identity thieves use stolen info?," May 24, 2017, https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[11] *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 (emphasis added).

69. For instance, with a stolen social security number, which is part of the Personal Information compromised in the Data Breach, someone can open financial, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[12] And with the information taken from Plaintiff, medical information and health insurance information, the cyber criminals can use that to qualify for expensive medical care and leave Maldonado and his contracted health insurer on the hook for massive medical bills.

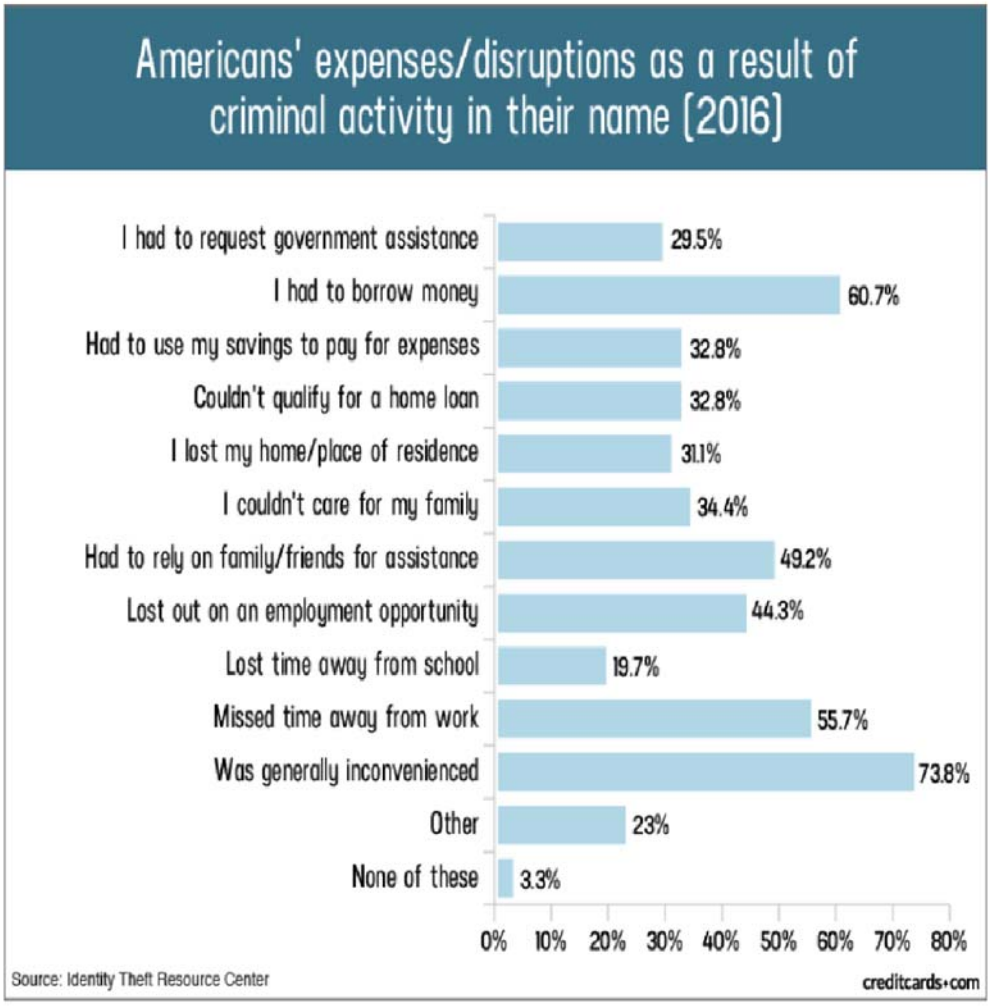
70. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[13]

71. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," said Pam Dixon, the founder and 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."[14]

72. If, moreover, the cyber criminals also received financial information, credit and debit cards, medical insurance information, driver's licenses and passports, as they did here, there is no limit to the amount of fraud that Solara has exposed the Breach Victims to.

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

73. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Personal and Medical Information such as that compromised in the Data Breach:[15]



Plaintiff and the Class have experienced one or more of these harms as a result of the Data Breach.

74. 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.[16] Almost half of medical identity

[15] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.
[16] *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.[17]

75. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[18]

76. Defendant's offer of one year of identity monitoring to Plaintiff and the Class is woefully inadequate. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal and Medical Information is stolen and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.* fraudulent acquisition and use of another person's Personal and Medical Information)-it does not prevent identity theft.[19]

77. 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 now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

78. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

[17] *Id.*
[18] "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.
[19] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost* by Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

a. Trespass, damage to and theft of 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 and having been already misused;

d. Damages flowing from Defendant untimely and inadequate notification of the data breach;

e. Loss of privacy suffered as a result of the data breach;

f. Ascertainable losses in the form of out-of-pocket expenses and 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 customers' personal information for which there is a well-established and quantifiable national and international market;

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

i. Damage to their credit due to fraudulent use of their Personal and Medical Information; and

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

79. Moreover, Plaintiff and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

80. Defendant itself acknowledged the harm caused by the data breach because it offered Plaintiff and Class Members twelve months of identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is woefully inadequate to protect Plaintiffs and Class Members from a

lifetime of identity theft risk and does nothing to reimburse Plaintiffs and Class Members for the injuries they have already suffered.

V. CLASS ALLEGATIONS

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

82. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a) and 23(b)(3), Plaintiff asserts all claims on behalf of a nationwide class, defined as follows:

All persons whose Personal and Medical Information was compromised by the Data Breach.

83. Excluded from the Class are 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 the members of their immediate families and judicial staff.

84. Alternatively, Plaintiff proposes the following subclasses by state or groups of states, defined as follows:

Statewide [name of State] Class: All residents of [name of State] whose Personal and Medical Information was compromised by the Data Breach.

A. CLASS CERTIFICATION IS APPROPRIATE

85. The proposed Nationwide Class or, alternatively, the separate Statewide Classes (collectively, the "Class" as used in this sub-section) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

86. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Although Defendant has not yet disclosed the full number of individuals affected by the Data Breach, upon information and believe, it numbers in the thousands.

87. **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 failed to adequately safeguard Plaintiff's and the Class' Personal and Medical Information;

b. Whether Defendant failed to protect Plaintiff's and the Class' Personal and Medical Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and the Class' Personal and Medical Information violated HIPAA, CMIA, and/or state laws and/or Defendant's other duties;

d. Whether Defendant violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

e. Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Breach Victims' Personal and Medical Information properly and as promised;

g. Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Personal and Medical Information;

h. Whether Defendant entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendant to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

i. Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state medical privacy statutes applicable to Plaintiff and the Class;

j. Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

k. Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

l. Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

m. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

88. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

89. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

90. **Risks of Prosecuting Separate Actions:** This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the

Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant are still in possession of Personal and Medical Information of Plaintiff and the Class, and Defendant's systems are still vulnerable to attack—one standard of conduct is needed to ensure the future safety of Personal and Medical Information in Defendant's possession.

91. **Policies Generally Applicable to the Class:** This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

92. **Superiority:** This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

A. COUNT I – NEGLIGENCE

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

94. Defendant solicited, gathered, and stored the Personal and Medical Information of Plaintiff and the Class.

95. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal and Medical Information of Plaintiff and the Class and the importance of adequate security.

96. Defendant were well aware of the fact that hackers routinely attempted to access Personal and Medical Information without authorization. Defendant also knew about numerous, well-publicized data breaches wherein hackers stole the Personal and Medical Information from companies who held or stored such information.

97. Defendant owed duties of care to Plaintiff and the Class whose Personal and Medical Information was entrusted to it. Defendant's duties included the following:

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

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

c. To adequately and properly train its employees to avoid phishing emails;

d. To adequately and properly train its employees regarding how to properly and securely transmit and store Personal and Medical Information;

e. To implement processes to quickly detect a data breach, security incident, or intrusion; and

f. 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.

98. Because Defendant knew that a security incident, breach or intrusion upon its systems would potentially damage thousands of its current and/or former patients and employees, including Plaintiff and Class members, it had a duty to adequately protect their Personal and Medical Information.

99. Defendant owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

100. Defendant knew, or should have known, that its security practices and computer systems did not adequately safeguard the Personal and Medical Information of Plaintiff and the Class.

101. Defendant breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard the Personal and Medical Information of Plaintiff and the Class.

102. Defendant breached their duties of care by failing to provide prompt notice of the Data Breach to the persons whose personal information was compromised.

103. Defendant acted with reckless disregard for the security of the Personal and Medical Information of Plaintiff and the Class because Defendant knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal and Medical Information that it collected and stored, which hackers were attempting to access.

104. Defendant acted with reckless disregard for the rights of Plaintiff and the Class by failing to provide prompt and adequate notice of the data breach so

that they could take measures to protect themselves from damages caused by the fraudulent use of Personal and Medical Information compromised in the Data Breach.

105. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendant with their personal information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect their systems (and the Personal and Medical Information that they stored on them) and to implement security practices to protect the Personal and Medical Information that they collected and stored from attack.

106. Defendant own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal and Medical Information. Defendant's misconduct included failing to:

a. Secure its employees' email accounts;
b. Secure access to its servers;
c. Comply with current industry standard security practices;
d. Encrypt Personal and Medical Information during transit and while stored on Defendant's systems;
e. Properly and adequately train their employees on proper data security practices;
f. Implement adequate system and event monitoring;
g. Implement the systems, policies, and procedures necessary to prevent hackers from accessing and utilizing Personal and Medical Information transmitted and/or stored by Defendant;
h. Undertake periodic audits of record-keeping processes to evaluate the safeguarding of Personal and Medical Information;
i. Develop a written records retention policy that identifies what information must be kept and for how long;

j. Destroy all discarded employee information, including information on prospective employees, temporary workers, subcontractor, and former employees;

k. Secure Personal and Medical Information and limit access to it to those with a legitimate business need;

l. Employ or contract with trained professionals to ensure security of network servers and evaluate the systems used to manage e-mail, Internet use, and so forth;

m. Avoid using Social Security numbers as a form of identification; and

n. Have a plan ready and in position to act quickly should a theft or data breach occur.

107. Defendant also had independent duties under federal and state law requiring them to reasonably safeguard Plaintiff's and the Class' Personal and Medical Information and promptly notify them about the Data Breach.

108. Defendant breached the duties they owed to Plaintiff and Class members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols and practices sufficient to protect their Personal and Medical Information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards before, during, and after the period of the Data Breach; and

d. By failing to timely and accurately disclose that the Personal and Medical Information of Plaintiff and the Class had been improperly acquired or accessed in the Data Breach.

109. But for Defendant wrongful and negligent breach of the duties it owed Plaintiff and the Class members, their Personal and Medical Information either would not have been compromised or they would have been able to prevent some or all of their damages.

110. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of further harm.

111. The injury and harm that Plaintiff and Class members suffered (as alleged above) was reasonably foreseeable.

112. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

113. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

B. COUNT II – NEGLIGENCE PER SE

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

115. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Personal and Medical Information of Plaintiff and the Class.

116. Pursuant to HIPAA's Privacy Rule and Security Rule, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and the Class's Personal and Medical Information.

117. Pursuant to the California CMIA, Defendant had additional duties to implement safeguards to protect Plaintiff's and the Class's Personal and Medical Information.

118. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Solara, 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.

119. Defendant solicited, gathered, and stored the Personal and Medical Information of Plaintiff and the Class as part of its business of manufacturing, selling, and installing gutter protection systems, which affects commerce.

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

121. Defendant breached its duties to Plaintiffs and the Class under the FTCA, HIPAA, CIMA, and other state data security and medical privacy statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Breach Victim's Personal and Medical Information.

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

123. Plaintiff and the Class are within the class of persons that the FTCA was intended to protect.

124. The harm that occurred as a result of the Data Breach is the type of harm the FTCA, HIPAA, and the state data breach and medical privacy statutes were intended to guard against.

125. 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' Personal and Medical Information.

126. Additionally, Defendant had a duty to promptly notify Breach Victims of the Data Breach For instance, California law requires that notice of a

"breach of the security of the system… shall be made in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82; *see also* 73 Pa. Stat. § 2303(a) (notice of any "breach of the security of the system" shall be made "without unreasonable delay").

127. Defendant notified all persons, regardless of which state they reside in, of the Data Breach on or about November 11, 2019.

128. Defendant knew on or before June 28, 2019, that unauthorized persons had accessed and/or viewed or were reasonably likely to have accessed and/or viewed private, protected, personal information of Plaintiff and the Class.

129. Defendant breached their duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiff and the Class of the Data Breach.

130. Defendant's violation of the FTCA, HIPAA, CMIA, state data security statutes, and/or the state data breach notification statutes constitute negligence *per se*.

131. 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 by, *inter alia*, having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place and renew a "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

132. 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*.

C. COUNT III – BREACH OF CONTRACT

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

134. As a direct-to-consumer medical device company, Defendant entered into contracts with Plaintiff and Class Members.

135. The promises and representations described above relating to compliance with HIPAA, CIMA, and industry practices, and about Solara's alleged concern for its patients privacy rights became terms of the contract between it and its customers, including Breach Victims.

136. Defendant breached these promises by failing to comply with HIPAA, CIMA, and reasonable industry practices.

137. As a result of Defendant's breach of these terms, Breach Victims have been seriously harmed and put at grave risk of debilitating future harms.

138. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

D. COUNT IV – BREACH OF IMPLIED CONTRACT (Alternatively to Count III)

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

140. When Plaintiff and the Class members provided their Personal and Medical Information to Defendant when seeking to purchase medical devices or seeking employment, they entered into implied contracts in which Defendant agreed to protect their Personal and Medical Information and timely notify them in the event of a data breach.

141. Defendant required its patients and employees provide Personal and Medical Information in order to purchase medical devises or to apply for a job with Defendant.

142. Defendant affirmatively represented that it collected and stored the Personal and Medical Information of Plaintiff and the members of the Class using reasonable, industry standard means.

143. Based on the 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.

144. 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 or provide timely notice of a data breach.

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

146. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' personal information and failing to provide them with timely and accurate notice of the Data Breach.

147. 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.

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

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

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

150. These promises and representations became a part of the contract between Solara and Breach Victims.

151. While Solara 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.

152. 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 unlawful practices by HIPAA and the CIMA.

153. Class Members did all or substantially all of the significant things that the contract required them to do.

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

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

156. Class Members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including overpayment for products and services, actual identity theft and/or imminent risk of devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term expense of attempting to mitigate and insure against these risks.

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

158. Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

F. COUNT VI – UNJUST ENRICHMENT

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

160. Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and Class Members either directly through copayments and coinsurance or indirectly through health insurance/medical plans that they had paid for.

161. Defendant had knowledge of the benefits conferred on it by Plaintiff and the Class Members.

162. The money that Plaintiffs and Class Members paid indirectly to Defendant was supposed to be used by Defendant, in part, to pay for the costs of HIPAA and CIMA compliance and reasonable data privacy and security practices and procedures.

163. As a result of Defendant's conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference in value between health care services with the reasonable data privacy and security practices and procedures that they paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

164. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or to adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

165. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received.

166. A constructive trust should be imposed on all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

G. COUNT VII – CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code § 17200, *et seq.*

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

168. Defendant violated 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 Cal. Bus. Prof. Code § 17200, including but not limited to the following:

a. Defendant engaged in deceptive acts and practices with regard to medical services provided to Plaintiff and Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard their Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they 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's Personal and Medical Information.

b. Defendant engaged in unfair acts and practices with respect to medical services by establishing the substandard security practices and procedures described herein; 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. These unfair acts and practices were immortal unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d et seq., CMIA, Cal. Civ. Code § 56, et seq., and California's data breach statute, Cal. Civ. Code § 1798.81.5.

c. Defendant's engaged in unfair acts and practices with respect to the sale of medical supplies by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

d. Defendant engaged in unlawful business practices by violating the privacy and security requirements of HIPAA, 42 U.S.C. § 1302d, et seq.

e. Defendant engaged in unlawful business practices by violating California's CMIA, Cal. Civ. Code § 56, et seq.

f. Defendant engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

169. 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.

170. 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 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.

171. Plaintiff seeks relief under Cal. Bus. & Prof. Code § 17200, e seq., 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. Pro. § 1021.5), and injunctive or other equitable relief.

H. COUNT VIII - PENNSYLVANIA UNFAIR TRADE PRACTICES, 73 Pa. Stat. Ann. § 201-1, et seq. (Brought on Behalf of an Alternative Pennsylvania Class)

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

173. Plaintiff brings this claim against Defendant on behalf of an alternative Pennsylvania Class.

174. Plaintiff and the alternative Pennsylvania Class directly or indirectly purchased medical supplies from Defendant in "trade" and "commerce" as defined in 73 Pa. Stat. Ann. § 201-2 for personal, family, and/or household purposes.

175. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiff and the alternative Pennsylvania Class in violation of 73 Pa. Stat. Ann. § 201-3, including but not limited to the following:

a. Defendant misrepresented material facts pertaining to the sale of medical supplies to the alternative Pennsylvania Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard the Personal and Medical Information of the alternative Pennsylvania Class from unauthorized disclosure, release, data breach, and theft in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi).

b. Defendant misrepresented material facts pertaining to the sale of medical supplies to the alternative Pennsylvania Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the alternative Pennsylvania Class's Personal and Medical Information in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi).

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the alternative Class's Personal and Medical Information in violation of in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi).

d. Defendant engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of medical supplies by failing to

maintain the privacy and security of the alternative Class's Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTCA, 15 U.S.C. § 45 and HIPAA, 42 U.S.C. § 1302d *et seq.*

e. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of medical supplies by failing to disclose the Data Breach to the alternative Class in a timely and accurate manner, in violation of 73 Pa. Stat. § 2303(a); and

f. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of medical supplies by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the alternative Class's Personal and Medical Information from further unauthorized disclosure, release, data breach, and theft.

176. The above unlawful, unfair, and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

178. As a direct and proximate result of Defendant's deceptive acts and practices, the alternative Class members suffered an ascertainable loss of money or property, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information.

179. The alternative Class seek relief under 73 Pa. Cons. Stat. § 201-9.2, including injunctive relief, actual damages or $100 per Class member, whichever greater, treble damages, and attorney fees and costs.

I. COUNT IX – CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code § 56 et seq.

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

181. Defendant is a "contractor," as defined in Cal. Civ. Code § 56.05(d), and "a provider of health care," as defined in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

182. 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 health care services from a provider of health care and to whom medical information pertains.").

183. 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).

184. 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 negligence failure to maintain or preserve medical information pertaining to Class Members in a manner that preserved the confidentiality of the information contained therein violates Cal. Civ. Code §§ 56.06 and 56.101(a).

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

186. Plaintiff and the Class were injured and have suffered damages 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 Civil 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.

J. COUNT X – INJUNCTIVE / DECLARATORY RELIEF

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

188. Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal and Medical Information it collected from Plaintiff and the Class.

189. Defendant owe a duty of care to Plaintiff and the members of the Class that requires them to adequately secure Personal and Medical Information.

190. Defendant still possess Personal and Medical Information regarding Plaintiff and members of the Class.

191. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted

the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

192. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's lax approach towards information security is known to hackers, the Personal and Medical Information in Defendant possession is even more vulnerable to cyberattack.

193. 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 the members of the Class are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendant's failure to address the security failings that lead to such exposure.

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

195. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. 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;

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

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

d. Ordering that Defendant's 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;

e. Ordering that Defendant cease transmitting Personal and Medical Information via unencrypted email;

f. Ordering that Defendant cease storing Personal and Medical Information in email accounts;

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

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

i. 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; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

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 damages, punitive damages, attorney fees, 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 as requested herein;

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 hereby demands a trial by jury on all appropriate issues raised in this Complaint.

DATED: November 29, 2019

GREEN & NOBLIN, P.C.

By: *s/ Robert S. Green*
Robert S. Green

2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

-and-

James R. Noblin
GREEN & NOBLIN, P.C.
4500 East Pacific Coast Highway
Fourth Floor
Long Beach, California 90804
Telephone: (562) 391-2487
Facsimile: (415) 477-6710

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
-and-
2926 Maple Ave., Ste. 200
Dallas, TX 75201
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com
Pro Hac Vice Application to be submitted

Cornelius P. Dukelow (OK Bar No. 19086)
ABINGTON COLE + ELLERY
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
Telephone and Facsimile: (918) 588-3400
Email:cdukelow@abingtonlaw.com
Pro Hac Vice Application to be submitted

Attorneys for Plaintiff

ClassAction.org