

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

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

5 **I. INTRODUCTION**

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

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

22 3. In short, thanks to Defendant's failure to protect the Breach Victims'
23 Personal and Medical Information, cyber criminals were able to steal everything
24 they could possibly need to commit nearly every conceivable form of identity theft
25 and wreak havoc on the financial and personal lives of potentially millions of
26 individuals.
27
28

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

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

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

23 7. Because Defendant presented such a soft target to cybercriminals,
24 Plaintiff and class members have been exposed to a heightened and imminent risk
25 of fraud and identity theft. Plaintiff and class members must now and in the future,
26 take their time to more closely monitor their financial accounts to guard against
27 identity theft.
28

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

4 9. On behalf of himself and all Breach Victims, Plaintiff seeks actual
5 damages, statutory damages, and punitive damages, with attorney fees, costs, and
6 expenses under the California Consumer Privacy Act, Cal. Civ. Code § 1798.80,
7 California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code §
8 56, other state personal and medical privacy laws, consumer protection and unfair
9 and deceptive practices acts, negligence, negligence per se, and breach of implied
10 contract. Plaintiff also seeks injunctive relief, including significant improvements
11 to Defendant's data security systems, future annual audits, and long-term credit
12 monitoring services funded by Defendant, and other remedies as the Court sees fit.

13 **II. THE PARTIES**

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

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

19 **III. JURISDICTION AND VENUE**

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

22 13. This Court has diversity jurisdiction over this action under the Class
23 Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving
24 more than 100 class members, the amount in controversy exceeds \$5,000,000,
25 exclusive of interest and costs, and many members of the class are citizens of
26 states different from Defendant.
27
28

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

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

8 **IV. FACTUAL ALLEGATIONS**

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

11 **Defendant**

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

16 18. As part of Defendant's business, Defendant collects substantial
17 amounts of Personal and Medical Information. The information Defendant collects
18 qualifies as "Personal information" under the California Customer Records Act,
19 Cal. Civ. Code § 1798.80, and other state data breach and information privacy
20 acts, including the Pennsylvania Breach of Personal Information Notification Act,
21 73 Pa. Stat. § 2302. The medical information that Defendant collects qualifies as
22 "Medical information" under the federal Health Information Portability and
23 Accountability Act (HIPAA), the California Confidentiality of Medical
24 Information Act (CMIA), Cal. Civ. Code § 56, *et seq.*, and other state medical
25 record protection acts.
26
27
28

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

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

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

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

16 28. After its “comprehensive manual and programmatic review,”
17 Defendant determined that:

18 The personal information present in the accounts at the time of the
19 incident varied by individual but may have included first and last names
20 and one or more of the following data elements: name, address, date of
21 birth, Social Security number, Employee Identification Number, medical
22 information, health insurance information, financial information, credit /
23 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

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

26
27
28
¹ “Solara Medical Supplies Provides Notice of a Data Breach,” PR Newswire, Nov. 13, 2019, <https://www.prnewswire.com/news-releases/solara-medical-supplies-provides-notice-of-a-data-breach-300957962.html>.

² *Id*

³ *Id*

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

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

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

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

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

23 34. Indeed, as discussed below, Solara promised patients that it would do
24 just that.
25
26
27
28

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 you⁵

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).

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

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

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

11 41. Defendant is a "business associate" covered by HIPPA. As such, it is
 12 required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part
 13 160 and Part 164.

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

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

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

24 45. "Electronic protected health information" is "individually identifiable
 25 health information . . . that is (i) Transmitted by electronic media; maintained in
 26 electronic media." 45 C.F.R. § 160.103.

27 46. HIPAA's Security Rule requires Defendant to do the following:
 28

- 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.

1 51. In addition to their obligations under federal and state laws,
2 Defendant owed a duty to Breach Victims whose Personal and Medical
3 Information was entrusted to Defendant to exercise reasonable care in obtaining,
4 retaining, securing, safeguarding, deleting, and protecting the Personal and
5 Medical Information in its possession from being compromised, lost, stolen,
6 accessed, and misused by unauthorized persons. Defendant owed a duty to Breach
7 Victims to provide reasonable security, including consistency with industry
8 standards and requirements, and to ensure that its computer systems and networks,
9 and the personnel responsible for them, adequately protected the Personal and
10 Medical Information of the Breach Victims.

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

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

21 54. Defendant owed a duty to Breach Victims whose Personal and
22 Medical Information was entrusted to Defendant to implement processes that
23 would detect a breach on its data security systems in a timely manner.
24

25 55. Defendant owed a duty to Breach Victims whose Personal and
26 Medical Information was entrusted to Defendant to act upon data security
27 warnings and alerts in a timely fashion.
28

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

5 57. Defendant owed a duty to Breach Victims whose Personal and
6 Medical Information was entrusted to Defendant to disclose if its computer
7 systems and data security practices were inadequate to safeguard individuals'
8 Personal and Medical Information from theft because such an inadequacy would
9 be a material fact in the decision to entrust Personal and Medical Information with
10 Defendant.

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

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

16
17 **D. Defendant Was on Notice of Cyber Attack Threats and the**
18 **Inadequacy of Its Data Security**

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

21 61. Defendant was on notice that the FBI has been concerned about data
22 security in the healthcare industry. In August 2014, after a cyberattack on
23 Community Health Systems, Inc., the FBI warned companies within the
24 healthcare industry that hackers were targeting them. The warning stated that
25 "[t]he FBI has observed malicious actors targeting healthcare related systems,
26
27
28

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 "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").

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

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

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

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

17 68. Hackers may not use the information right away. According to the
 18 U.S. Government Accountability Office, which conducted a study regarding data
 19 breaches:
 20

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

27
 28 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.html> (emphasis added).

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

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

14 71. "Medical identity theft is a growing and dangerous crime that leaves
15 its victims with little to no recourse for recovery," said Pam Dixon, the founder
16 and executive director of World Privacy Forum. "Victims often experience
17 financial repercussions and worse yet, they frequently discover erroneous
18 information has been added to their personal medical files due to the thief's
19 activities."¹⁴

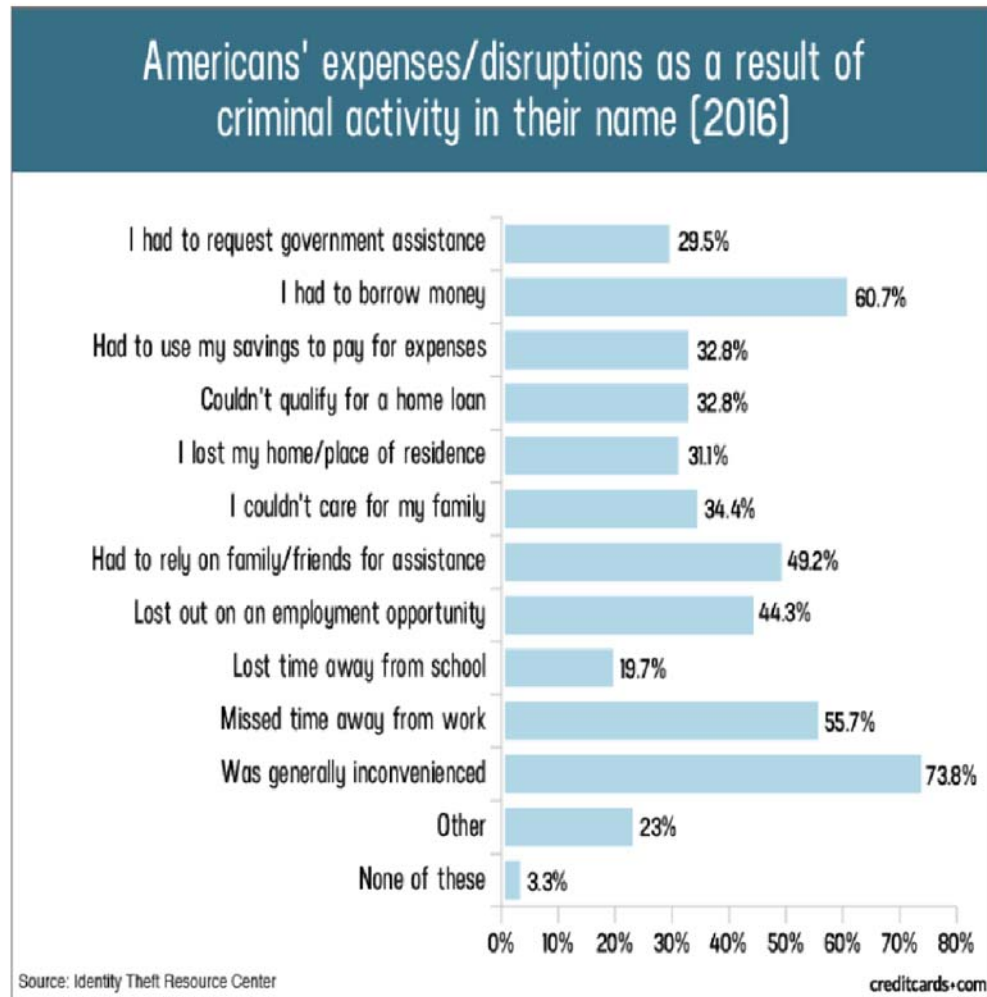
20 72. If, moreover, the cyber criminals also received financial information,
21 credit and debit cards, medical insurance information, driver's licenses and
22 passports, as they did here, there is no limit to the amount of fraud that Solara has
23 exposed the Breach Victims to.
24
25
26
27

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-identity-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/>.

1 theft victims lose their healthcare coverage as a result of the incident, while nearly
2 one-third saw their insurance premiums rise, and forty percent were never able to
3 resolve their identity theft at all.¹⁷

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

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

13 77. As a direct and proximate result of the Data Breach, Plaintiff and the
14 Class have been placed at an imminent, immediate, and continuing increased risk
15 of harm from fraud and identity theft. Plaintiff and the Class now have to take the
16 time and effort to mitigate the actual and potential impact of the Data Breach on
17 their everyday lives, including placing "freezes" and "alerts" with credit reporting
18 agencies, contacting their financial institutions, closing or modifying financial
19 accounts, and closely reviewing and monitoring bank accounts and credit reports
20 for unauthorized activity for years to come.

21 78. Plaintiff and the Class have suffered, and continue to suffer,
22 economic damages and other actual harm for which they are entitled to
23 compensation, including:
24
25
26
27

28 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.cnn.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.

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

- 5 a. Whether Defendant failed to adequately safeguard Plaintiff's
 6 and the Class' Personal and Medical Information;
- 7 b. Whether Defendant failed to protect Plaintiff's and the Class'
 8 Personal and Medical Information;
- 9 c. Whether Defendant's email and computer systems and data
 10 security practices used to protect Plaintiff's and the Class'
 11 Personal and Medical Information violated HIPAA, CMIA,
 12 and/or state laws and/or Defendant's other duties;
- 13 d. Whether Defendant violated the data security statutes and data
 14 breach notification statutes applicable to Plaintiff and the
 15 Class;
- 16 e. Whether Defendant failed to notify Plaintiff and members of
 17 the Class about the Data Breach expeditiously and without
 18 unreasonable delay after the Data Breach was discovered;
- 19 f. Whether Defendant engaged in unfair, unlawful, or deceptive
 20 practices by failing to safeguard Breach Victims' Personal and
 21 Medical Information properly and as promised;
- 22 g. Whether Defendant acted negligently in failing to safeguard
 23 Plaintiff's and the Class' Personal and Medical Information;
- 24 h. Whether Defendant entered into implied contracts with
 25 Plaintiff and the members of the Class that included contract
 26 terms requiring Defendant to protect the confidentiality of
 27 Personal and Medical Information and have reasonable
 28 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

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

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

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

1 **VI. CAUSES OF ACTION**

2 **A. COUNT I – NEGLIGENCE**

3
4 93. Plaintiff incorporates by reference all allegations of the preceding
5 paragraphs as though fully set forth herein.

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

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

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

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

- 19 a. To exercise reasonable care in obtaining, retaining, securing,
20 safeguarding, deleting and protecting the Personal and Medical
21 Information in its possession;
- 22 b. To protect the Personal and Medical Information in its possession
23 using reasonable and adequate security procedures and systems;
- 24 c. To adequately and properly train its employees to avoid phishing
25 emails;
- 26 d. To adequately and properly train its employees regarding how to
27 properly and securely transmit and store Personal and Medical
28 Information;

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

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

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

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

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

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

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

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

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

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

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

11 106. Defendant own conduct also created a foreseeable risk of harm to
12 Plaintiff and Class members and their Personal and Medical Information.

13 Defendant's misconduct included failing to:

- 14 a. Secure its employees' email accounts;
- 15 b. Secure access to its servers;
- 16 c. Comply with current industry standard security practices;
- 17 d. Encrypt Personal and Medical Information during transit and while
18 stored on Defendant's systems;
- 19 e. Properly and adequately train their employees on proper data security
20 practices;
- 21 f. Implement adequate system and event monitoring;
- 22 g. Implement the systems, policies, and procedures necessary to prevent
23 hackers from accessing and utilizing Personal and Medical
24 Information transmitted and/or stored by Defendant;
- 25 h. Undertake periodic audits of record-keeping processes to evaluate the
26 safeguarding of Personal and Medical Information;
- 27 i. Develop a written records retention policy that identifies what
28 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.

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

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

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

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

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

15 **B. COUNT II – NEGLIGENCE PER SE**

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

18 115. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C.
 19 § 45, Defendant had a duty to provide fair and adequate computer systems and
 20 data security to safeguard the Personal and Medical Information of Plaintiff and
 21 the Class.

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

25 117. Pursuant to the California CMIA, Defendant had additional duties to
 26 implement safeguards to protect Plaintiff's and the Class's Personal and Medical
 27 Information.
 28

1 118. The FTCA prohibits “unfair . . . practices in or affecting commerce,”
2 including, as interpreted and enforced by the FTC, the unfair act or practice by
3 businesses, such as Solara, of failing to use reasonable measures to protect
4 Personal and Medical Information. The FTC publications and orders described
5 above also formed part of the basis of Defendant’s duty in this regard.

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

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

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

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

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

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

23 125. Defendant breached its duties to Plaintiff and the Class under these
24 laws by failing to provide fair, reasonable, or adequate computer systems and data
25 security practices to safeguard Plaintiff’s and the Class’ Personal and Medical
26 Information.

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

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

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

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

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

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

16 131. As a direct and proximate result of Defendant’s negligence *per se*,
17 Plaintiff and the Class have suffered, and continue to suffer, damages arising from
18 the Data Breach by, *inter alia*, having to spend time reviewing their accounts and
19 credit reports for unauthorized activity; spend time and incur costs to place and re-
20 new a “freeze” on their credit; be inconvenienced by the credit freeze, which
21 requires them to spend extra time unfreezing their account with each credit bureau
22 any time they want to make use of their own credit; and becoming a victim of
23 identity theft, which may cause damage to their credit and ability to obtain
24 insurance, medical care, and jobs.

25 132. The injury and harm that Plaintiff and Class members suffered (as
26 alleged above) was the direct and proximate result of Defendant’s negligence *per*
27 *se*.

1 **C. COUNT III – BREACH OF CONTRACT**

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

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

6 135. The promises and representations described above relating to
7 compliance with HIPAA, CIMA, and industry practices, and about Solara's
8 alleged concern for its patients privacy rights became terms of the contract
9 between it and its customers, including Breach Victims.
10

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

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

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

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

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

22 140. When Plaintiff and the Class members provided their Personal and
23 Medical Information to Defendant when seeking to purchase medical devices or
24 seeking employment, they entered into implied contracts in which Defendant
25 agreed to protect their Personal and Medical Information and timely notify them in
26 the event of a data breach.
27
28

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

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

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

10 144. Plaintiff and Class members would not have provided their Personal
11 and Medical Information to Defendant had they known that Defendant would not
12 safeguard their Personal and Medical Information as promised or provide timely
13 notice of a data breach.

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

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

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

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

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

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

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

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

6 152. Defendant breached this implied covenant when it engaged in acts
7 and/or omissions that are declared unfair trade practices by the FTC and state
8 statutes and regulations, and unlawful practices by HIPAA and the CIMA.

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

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

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

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

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

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

1 **F. COUNT VI – UNJUST ENRICHMENT**

2 159. Plaintiff incorporates by reference all allegations of the preceding
3 paragraphs as though fully set forth herein.
4

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

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

11 162. The money that Plaintiffs and Class Members paid indirectly to
12 Defendant was supposed to be used by Defendant, in part, to pay for the costs of
13 HIPAA and CIMA compliance and reasonable data privacy and security practices
14 and procedures.
15

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

21 164. Under principals of equity and good conscience, Defendant should
22 not be permitted to retain the money belonging to Plaintiff and Class Members
23 because Defendant failed to implement (or to adequately implement) the data
24 privacy and security practices and procedures that Plaintiff and Class Members
25 paid for and that were otherwise mandated by HIPAA regulations, federal, state,
26 and local laws, and industry standards.
27
28

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

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

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

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

10 168. Defendant violated Cal. Bus. Prof. Code § 17200 *et seq.* by engaging
11 in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive,
12 untrue or misleading advertising that constitute acts of "unfair competition" as
13 defined in Cal. Bus. Prof. Code § 17200, including but not limited to the
14 following:

- 15 a. Defendant engaged in deceptive acts and practices with regard to
16 medical services provided to Plaintiff and Class by representing
17 and advertising that they would maintain adequate data privacy
18 and security practices and procedures to safeguard their Personal
19 and Medical Information from unauthorized disclosure, release,
20 data breach, and theft; representing and advertising that they did
21 and would comply with the requirement of relevant federal and
22 state laws pertaining to the privacy and security of the Class's
23 Personal and Medical Information; and omitting, suppressing,
24 and concealing the material fact of the inadequacy of the privacy
25 and security protections for the Class's Personal and Medical
26 Information.
27
28

- 1 b. Defendant engaged in unfair acts and practices with respect to
2 medical services by establishing the substandard security
3 practices and procedures described herein; by soliciting and
4 collecting Class members' Personal and Medical Information
5 with knowledge that the information would not be adequately
6 protected; and by storing Plaintiff's and Class members' Personal
7 and Medical Information in an unsecure electronic environment.
8 These unfair acts and practices were immoral unethical,
9 oppressive, unscrupulous, unconscionable, and/or substantially
10 injurious to Plaintiff and Class members. Defendant's practice
11 was also contrary to legislatively declared and public policies
12 that seek to protect consumer data and ensure that entities who
13 solicit or are entrusted with personal data utilize appropriate
14 security measures, as reflected by laws like the FTCA, 15 U.S.C.
15 § 45, HIPAA, 42 U.S.C. § 1302d et seq., CMIA, Cal. Civ. Code
16 § 56, et seq., and California's data breach statute, Cal. Civ. Code
17 § 1798.81.5.
- 18 c. Defendant's engaged in unfair acts and practices with respect to
19 the sale of medical supplies by failing to disclose the Data
20 Breach in a timely and accurate manner, contrary to the duties
21 imposed by Cal. Civ. Code § 1798.82.
- 22 d. Defendant engaged in unlawful business practices by violating
23 the privacy and security requirements of HIPAA, 42 U.S.C. §
24 1302d, et seq.
- 25 e. Defendant engaged in unlawful business practices by violating
26 California's CMIA, Cal. Civ. Code § 56, et seq.
- 27
- 28

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

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

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

15 171. Plaintiff seeks relief under Cal. Bus. & Prof. Code § 17200, e seq.,
16 including restitution to the Class of money or property that the Defendant may
17 have acquired by means of Defendant's deceptive, unlawful, and unfair business
18 practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal.
19 Code Civ. Pro. § 1021.5), and injunctive or other equitable relief.

20
21 **H. COUNT VIII - PENNSYLVANIA UNFAIR TRADE**
22 **PRACTICES, 73 Pa. Stat. Ann. § 201-1, et seq. (Brought on**
23 **Behalf of an Alternative Pennsylvania Class)**

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

26 173. Plaintiff brings this claim against Defendant on behalf of an
27 alternative Pennsylvania Class.
28

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

4 175. Defendant engaged in unlawful, unfair, and deceptive acts and
5 practices, misrepresentations, and the concealment, suppression, and omission of
6 material facts with respect to the sale and advertisement of the services purchased
7 by Plaintiff and the alternative Pennsylvania Class in violation of 73 Pa. Stat. Ann.
8 § 201-3, including but not limited to the following:

- 9
- 10 a. Defendant misrepresented material facts pertaining to the sale of
11 medical supplies to the alternative Pennsylvania Class by
12 representing that they would maintain adequate data privacy and
13 security practices and procedures to safeguard the Personal and
14 Medical Information of the alternative Pennsylvania Class from
15 unauthorized disclosure, release, data breach, and theft in violation
16 of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi).
- 17 b. Defendant misrepresented material facts pertaining to the sale of
18 medical supplies to the alternative Pennsylvania Class by
19 representing that they did and would comply with the
20 requirements of relevant federal and state laws pertaining to the
21 privacy and security of the alternative Pennsylvania Class's
22 Personal and Medical Information in violation of 73 Pa. Stat. Ann.
23 § 201-3(4)(v), (ix), and (xxi).
- 24 c. Defendant omitted, suppressed, and concealed the material fact of
25 the inadequacy of the privacy and security protections for the
26 alternative Class's Personal and Medical Information in violation
27 of in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi).
- 28 d. Defendant engaged in unfair, unlawful, and deceptive acts and
practices with respect to the sale of medical supplies by failing to

1 maintain the privacy and security of the alternative Class's
 2 Personal and Medical Information, in violation of duties imposed
 3 by and public policies reflected in applicable federal and state
 4 laws, resulting in the Data Breach. These unfair, unlawful, and
 5 deceptive acts and practices violated duties imposed by laws
 6 including the FTCA, 15 U.S.C. § 45 and HIPAA, 42 U.S.C.
 7 § 1302d *et seq.*

- 8 e. Defendant engaged in unlawful, unfair, and deceptive acts and
 9 practices with respect to the sale of medical supplies by failing to
 10 disclose the Data Breach to the alternative Class in a timely and
 11 accurate manner, in violation of 73 Pa. Stat. § 2303(a); and
 12 f. Defendant engaged in unlawful, unfair, and deceptive acts and
 13 practices with respect to the sale of medical supplies by failing to
 14 take proper action following the Data Breach to enact adequate
 15 privacy and security measures and protect the alternative Class's
 16 Personal and Medical Information from further unauthorized
 17 disclosure, release, data breach, and theft.

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

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

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

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

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

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

13 181. Defendant is a "contractor," as defined in Cal. Civ. Code § 56.05(d),
14 and "a provider of health care," as defined in Cal. Civ. Code § 56.06, and is
15 therefore subject to the requirements of the California Confidentiality of Medical
16 Information Act (CMIA), Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b),
17 56.101(a) and (b).

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

22 183. Defendant disclosed "medical information," as defined in CMIA, Cal.
23 Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in
24 violation of Cal. Civ. Code § 56.10(a).

25 184. Defendant's negligence resulted in the release of individually-
26 identifiable medical information pertaining to Plaintiff and the Class to
27 unauthorized persons and the breach of the confidentiality of that information.
28

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

4 185. Defendant's computer systems did not protect and preserve the
5 integrity of electronic medical information in violation of Cal. Civ. Code §
6 56.101(b)(1)(A).

7
8 186. Plaintiff and the Class were injured and have suffered damages from
9 Defendant's illegal disclosure and negligent release of their medical information in
10 violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under
11 Civil Code §§ 56.35 and 56.36, including actual damages, nominal statutory
12 damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorney
13 fees, expenses and costs.

14 **J. COUNT X – INJUNCTIVE / DECLARATORY RELIEF**

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

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

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

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

24 191. Since the Data Breach, Defendant has announced few if any changes
25 to their data security infrastructure, processes or procedures to fix the
26 vulnerabilities in their computer systems and/or security practices which permitted
27
28

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

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

7 193. Actual harm has arisen in the wake of the Data Breach regarding
8 Defendant's contractual obligations and duties of care to provide security measures
9 to Plaintiff and the members of the Class. Further, Plaintiff and the members of
10 the Class are at risk of additional or further harm due to the exposure of their
11 Personal and Medical Information and Defendant's failure to address the security
12 failings that lead to such exposure.

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

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

- 21
- 22 a. Ordering that Defendant engage third-party security
23 auditors/penetration testers as well as internal security personnel
24 to conduct testing, including simulated attacks, penetration tests,
25 and audits on Defendant's systems on a periodic basis, and
26 ordering Defendant to promptly correct any problems or issues
27 detected by such third-party security auditors;
28

- 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.

////

////

////

////

////

////

////

1 **VIII. DEMAND FOR JURY TRIAL**

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

4 DATED: November 29, 2019

GREEN & NOBLIN, P.C.

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

7 2200 Larkspur Landing Circle, Suite 101
8 Larkspur, CA 94939
9 Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

10 -and-

11 James R. Noblin
12 **GREEN & NOBLIN, P.C.**
13 4500 East Pacific Coast Highway
14 Fourth Floor
15 Long Beach, California 90804
Telephone: (562) 391-2487
Facsimile: (415) 477-6710

16 William B. Federman
17 **FEDERMAN & SHERWOOD**
18 10205 N. Pennsylvania Ave.
19 Oklahoma City, OK 73120
20 -and-
21 2926 Maple Ave., Ste. 200
22 Dallas, TX 75201
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

Pro Hac Vice Application to be submitted

23 Cornelius P. Dukelow (OK Bar No. 19086)
24 **ABINGTON COLE + ELLERY**
25 320 South Boston Avenue, Suite 1130
26 Tulsa, Oklahoma 74103
27 Telephone and Facsimile: (918) 588-3400
Email: cdukelow@abingtonlaw.com
Pro Hac Vice Application to be submitted

28 *Attorneys for Plaintiff*

CIVIL COVER SHEET

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

19CV2284 H KSC

I. (a) PLAINTIFFS

Juan Maldonado, individually and on behalf of all others similarly situated.

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

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

Robert S. Green/James Robert Noblin
Green & Noblin, P.C. / (562) 397-2487
4500 E. Pacific Coast Hwy., 4th Floor, Long Beach, CA 90804

DEFENDANTS

Solara Medical Supplies, LLC.

County of Residence of First Listed Defendant San Diego County, CA
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys (If Known)

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

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

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

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|---------------------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input checked="" type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

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

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input checked="" type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

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

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

VI. CAUSE OF ACTION

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

28 U.S.C. § 1332(d)

Brief description of cause:

Data breach of medical information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

11/29/2019

SIGNATURE OF ATTORNEY OF RECORD

s/ Robert S. Green

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

EXHIBIT 1



85 1 18492 *****AUTO**ALL FOR AADC 190

JUAN MALDONADO

6012 KEYSTONE ST

PHILADELPHIA, PA 19135-4218



November 11, 2019

Re: Notice of Data Breach

Dear Juan Maldonado,

Solara Medical Supplies, LLC ("Solara") is writing to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On June 28, 2019, Solara determined that an unknown actor gained access to a limited number of employee Office 365 accounts, from April 2, 2019 to June 20, 2019, as a result of a phishing email campaign. We worked with third party forensic experts to investigate and respond to this incident and confirm the security of relevant Solara systems. Through this investigation we determined that certain information present within the employee Office 365 accounts may have been accessed or acquired by an unknown actor at the time of the incident. We, therefore, undertook a comprehensive review of the accounts to identify potentially affected personal information. Our review determined that some of your personal information was present in an affected account at the time of the incident.

What Information Was Involved? The investigation determined that some of your personal information was present in an affected account at the time of the incident including your name, date of birth, medical information, and health insurance information. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant Solara systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the email accounts to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

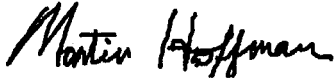
Solara notified law enforcement of this incident and is notifying relevant state and federal regulators. We are also offering you access to complimentary identity monitoring services for twelve (12) months through Kroll. These services include credit monitoring, fraud consultation and identity theft restoration services. If you wish to activate the identity monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Your Information*. There you will also find more information on the identity monitoring services we are making available to you. While Solara will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-877-460-0157 (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to Solara at: 2084 Otay Lakes Rd #102, Chula Vista, CA 91913 or visit <https://www.solara.com/dataincident>.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink that reads "Martin Hoffman". The signature is written in a cursive, slightly slanted style.

Martin Hoffman
Vice President of Compliance and Legal
Solara Medical Supplies, LLC

Activate Your Complimentary Identity Monitoring

To activate Kroll's identity monitoring, fraud consultation, and identity theft restoration services, please follow the steps below:

- 1) Visit **krollbreach.idMonitoringService.com** to activate.
- 2) You have until **February 7, 2020** to activate your identity monitoring services. **Your membership number will not work after this date.**
- 3) Provide your personal information to Kroll, as requested.
- 4) Provide the following Membership Number: **C21255077**.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html**TransUnion**

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze**Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html**TransUnion**

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert**Equifax**

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 154 Rhode Island residents impacted by this incident.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.



A Division of
DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.