BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
PAULA M. ROACH (254142)
701 B Street, Suite 1700
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
tblood@bholaw.com
toreardon@bholaw.com
proach@bholaw.com

FEDERMAN & SHERWOOD
WILLLIAM B. FEDERMAN *
CARIN L. MARCUSSEN *
10205 N. Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Tel: 405/235-1560
405/239-2112 (fax)
wbf@federmanlaw.com
clm@federmanlaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

TERRI GREULICH, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MEDICAL INFORMATICS ENGINEERING, INC.,

Defendant.

Case No. '15CV1750 L MDD

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Terri Greulich ("Plaintiff"), individually and on behalf of the Classes defined below of similarly situated persons, alleges the following against Medical Informatics Engineering, Inc., ("MIE" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

SUMMARY OF ACTION

1. This action seeks redress for MIE's failure to secure and safeguard its users' Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively referred to herein as "Personal Information" or "PI"). On June 10, 2015, MIE disclosed a data breach involving the exposure of Personal Information of tens of thousands of individuals from around the United States (the "Security Breach"). MIE's security failures enabled intruders to access and seize the Personal Information from within MIE's systems.

2. According to MIE, the following PI of tens of thousands of individuals from around the United States was compromised in the Security Breach: name, telephone number, mailing address, username, hashed password, security question and answer, email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, spousal name, spousal date of birth, and child's name and birth statistics. As a result, Plaintiff's and Class members' PI is at serious and ongoing risk of misuse, including because the intruders may use the data they obtained as a result of MIE's inadequate security to exploit Plaintiff and Class members throughout the country.

3. Plaintiff retains a significant interest in ensuring that her PI is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose PI was accessed and seized as a result of the Security Breach. Plaintiff asserts claims against MIE for

violations of state data breach statutes, negligence, and breach of implied contract. Plaintiff, on behalf of herself and similarly situated consumers, seeks to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a recurrence of the data breach and resulting injury, restitution, disgorgement and reasonable costs and attorneys' fees.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

5. This Court has personal jurisdiction over Defendant because it regularly conducts business in California. Defendant intentionally avails itself of this jurisdiction by marketing and selling products in California and by conducting business in California with certain of the members of the Classes. Defendant has sufficient minimum contacts with California to render the exercise of jurisdiction by this court permissible.

6. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a) and (b) because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

7. Plaintiff realleges, as if fully set forth, each and every allegation herein.

8. Plaintiff Terri Greulich is a resident of San Diego, California. On or about July 27, 2015, Plaintiff Greulich received a letter from MIE dated July 17, 2015, notifying her of the Security Breach. The July 17, 2015 letter from MIE stated that Plaintiff Greulich's Personal Information was compromised in the Security Breach.

9. Plaintiff and each Class member suffered actual injury from having his or her PI accessed and seized in and as a result of the MIE Security Breach.

10. Plaintiff and each Class member suffered actual injury in the form of damages to and diminution in the value of his or her PI – a form of intangible property that Plaintiff and each Class member entrusted to MIE and that was accessed and seized in and as a result of the MIE Security Breach.

11. Plaintiff and each Class members has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his or her PI being placed in the hands of criminals via sale of Plaintiff's and Class members' PI on the Internet black market. Plaintiff has a continuing interest in ensuring that her PI, which remains in the possession of MIE, is protected and safeguarded from future breaches.

12. Defendant Medical Informatics Engineering, Inc. is an Indiana corporation headquartered in Fort Wayne, Indiana.

STATEMENT OF FACTS

13. MIE operates a health information exchange software platform that allows for the electronic movement of information among disparate health care information systems while maintaining the integrity and meaning of the information being exchanged. As part of its business, MIE stores vast amounts of Personal Information of individuals throughout the United States.

14. The PI stored by MIE includes, but is not necessarily limited to: name, telephone number, mailing address, username, hashed password, security question and answer, email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, spousal name, spousal date of birth, and child's name and birth statistics.

15. On information and belief, an untold number of individuals became the victims of the Security Breach when their PI was accessed and seized from

MIE's information systems. According to MIE, the following user information was compromised in the Security Breach: name, telephone number, mailing address, username, hashed password, security question and answer, email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, spousal name, spousal date of birth, and child's name and birth statistics.

16. According to MIE, the Security Breach began on or about May 7, 2015, and was first discovered on or about May 26, 2015.

17. MIE publicly announced the Security Breach on June 10, 2015.

18. MIE sent data breach notification letters dated July 17, 2015, to affected individuals throughout the United States.

19. MIE's failure to comply with reasonable security standards provided MIE with short-term and fleeting benefits in the form of saving on the costs of adequate security, but at the expense and to the severe detriment of MIE's own users – including Plaintiff and Class members here – who have been subject to the Security Breach or otherwise have had their PI accessed and seized and placed at serious and ongoing risk.

20. MIE allowed widespread and systematic access and seizure of its users' PI. MIE's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect the Personal Information in its care.

Security Breaches Lead to Identity Theft

21. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[1] As the GAO Report states, this

[1] *See* U.S. Gov't Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited,*

type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft "face substantial costs and time to repair the damage to their good name and credit record."[2]

22. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history and reputation and can take time, money and patience to resolve.[3] Identity thieves use stolen PI for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

23. A person whose PI has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

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

Id. at 2a.

///

///

However, the Full Extent Is Unknown (GAO-07-737), available at http://www.gao.gov/new.items/d07737.pdf (last visited August 8, 2015).

[2] *Id*. at 2.

[3] *See* US Federal Trade Commission and United States of America, *Taking Charge: What to Do If Your Identity is Stolen*, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited August 8, 2015).

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

Personal Information is Valuable Property

24. At a FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PI as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy.
>
> Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

25. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as Personal Information functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

26. The FTC has also recognized that PI is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[7]

27. Recognizing the high value that consumers place on their PI, many companies now offer consumers an opportunity to sell this information to

---

[5] Federal Trade Commission, *The Information Marketplace: Merging and Exchanging Consumer Data*, *Conference and Workshop*, *Washington D.C.*, 28 (March 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited August 8, 2015).

[6] *See* J. Angwin and W. Steel, *Web's Hot New Commodity: Privacy*, The wall Street Journal, Feb. 28, 2001, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited August 8, 2015).

[7] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), (Dec. 7, 2009), *available at* https://www.ftc.gov/sites/default/files/ documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited August 8, 2015).

advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PI.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

28. Consumers place a high value not only on their PI, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

29. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their PI – the very injury at issue here – between $11.33 and $16.58 per website.[11]

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

///

---

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times, July 16, 2010, *available at* http://www.nytimes.com /2010/07/18/business /18unboxed.html (last visited August 8, 2015).

[9] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal, Feb. 28, 2011, *available at* http://online.wsj.com/article/ SB10001424052748703529004576160764037920274.html (last visited August 3, 2015).

[10] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), pre-publication version available at http://www.heinz.cmu.edu acquisti/papers/acquisti-onlinepurchasing-privacy.pdf (last visited August 8, 2015).

[11] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.200.6483&rep= rep1&type=pdf (emphasis added) (last visited August 3, 2015).

Damages Sustained by Plaintiff and the Class

31. A portion of the services purchased from MIE by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PI. Because Plaintiff and the Class were denied privacy protections that they were entitled to receive, Plaintiff and the Class have been damaged thereby.

32. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by MIE's wrongful conduct.

33. Moreover, as explained above, fraudulent use of PI might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

34. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their PI as a result of the Security Breach.

CLASS ALLEGATIONS

35. Pursuant to Fed. R. Civ. P. 23, Plaintiff asserts her claims that MIE violated state data breach notification statutes (Count I) on behalf of separate statewide classes defined as follows:

> **Statewide Data Breach Notification Classes:**
> All residents of [name of State] whose Personal Information was compromised as a result of the data breach first disclosed by MIE in June 2015.

36. Plaintiff asserts the state data breach notification law claims (Count I) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon,

South Carolina, Tennessee, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia.

37. Pursuant to Fed. R. Civ. P. 23, Plaintiff asserts her common law claims for negligence (Count II) and breach of implied contract (Count III) on behalf of a nationwide class, defined as follows:

> **Nationwide Class:**
> All residents of the United States whose Personal Information was compromised as a result of the data breach first disclosed by MIE in June 2015.

38. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims for negligence (Count II) and breach of implied contract (Count III) under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

> **Statewide [Negligence or Breach of Implied Contract] Classes:**
> All residents of [name of State] whose Personal Information was compromised as a result of the data breach first disclosed by MIE in June 2015.

39. Pursuant to Fed. R. Civ. P.23, Plaintiff asserts claims under the California Customer Records Act, California Civil Code section 1798.81.5 (Count IV), the California Confidentiality of Medical Information Act, California Civil Code section 56 (Count V), and California's Unfair Competition Law, California Business and Professions Code section 17200 (Count VI) on behalf of a California class defined as follows:

> **California Class:**
> All residents of California whose Personal Information was compromised as a result of the data breach first disclosed by MIE in June 2015.

40. Excluded from each of the above Classes are Defendant and parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors,

successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

41. Each of the proposed classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

42. **Numerosity.** The proposed classes include hundreds of thousands of individuals whose PI was compromised in the Security Breach. While the precise number of Class members in each proposed class has not yet been determined, the massive size of the MIE Security Breach indicates that joinder of each member would be impracticable.

43. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. whether MIE engaged in the conduct alleged herein;

b. whether MIE had a legal duty to adequately protect Plaintiff's and Class members' Personal Information;

c. whether MIE breached its legal duty by failing to adequately protect Plaintiff's and Class members' Personal Information;

d. whether MIE had a legal duty to provide timely and accurate notice of the MIE Security Breach to Plaintiff and Class members;

e. whether MIE breached its duty to provide timely and accurate notice of the MIE Security Breach to Plaintiff and Class members;

f. whether and when MIE knew or should have known that its computer systems were vulnerable to attack;

g. whether Plaintiff and Class members are entitled to recover actual damages and/or statutory damages; and

h. whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

44. **Typicality.** Plaintiff's claims are typical of the claims of the Class. Plaintiff and Class members were injured through MIE's uniform misconduct and their legal claims arise from the same core MIE practices.

45. **Adequacy.** Plaintiff is an adequate representative of the proposed Classes because her interests do not conflict with the interests of the Class members she seeks to represent. Plaintiff's counsel are very experienced in litigating consumer class actions, data breach class actions and complex commercial disputes.

46. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against MIE. Even if it were economically feasible, requiring hundreds of thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

47. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). MIE has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

48. Finally, all members of the purposed Classes are readily ascertainable. MIE has access to addresses and other contact information for

hundreds of thousands of members of the Classes, which can be used to identify Class members.

COUNT I

VIOLATIONS OF STATE DATA BREACH NOTIFICATION STATUTES

(On Behalf of Plaintiff and the Separate Statewide Data Breach Statute Classes)

49. Plaintiff realleges, as if fully set forth, each and every allegation herein.

50. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

51. The MIE Security Breach constituted a breach that triggered the notice provisions of the data breach statutes and the Personal Information taken includes categories of personal information protected by the data breach statutes.

52. MIE unreasonably delayed in informing Plaintiff and members of the Statewide Data Breach Statute Classes ("Class," as used in this Count I), about the Security Breach after MIE knew or should have known that the Security Breach had occurred.

53. Plaintiff and Class members were damaged by MIE's failure to comply with the data breach statutes.

54. Had MIE provided timely and accurate notice, Plaintiff and Class members could have avoided or mitigated the harm caused by the Security Breach. For example, they could have taken earlier security precautions in time to prevent or minimize identity theft.

55. MIE's failure to provide timely and accurate notice of the MIE Security Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Cal. Civ. Code § 1798.80, *et seq.*;

c. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

d. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

e. D.C. Code § 28-3852(a), *et seq.*;

f. Ga. Code Ann. § 10-1-912(a), *et seq.*;

g. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

h. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

i. Iowa Code Ann. § 715C.2(1), *et seq.*;

j. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

k. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

l. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

m. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

n. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

o. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

p. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

q. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

r. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

s. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

t. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

u. S.C. Code Ann. § 39-1-90(A), *et seq.*;

v. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

w. Va. Code Ann. § 18.2-186.6(B), *et seq.*;

x. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

y. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

z. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

56. Plaintiff and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT II

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Separate Statewide Negligence Classes)

57. Plaintiff realleges, as if fully set forth, each and every allegation herein.

58. MIE owed numerous duties to Plaintiff and to members of the Nationwide Class, or, alternatively, members of the separate Statewide Negligence Classes (collectively, the "Class" as used in this Count). MIE's duties included the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PI in its possession;

b. to protect their PI using reasonable and adequate security procedures and systems that are consistent with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the MIE Security Breach.

59. MIE owed a duty of care not to subject the PI of Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. MIE solicited, gathered,

and stored Plaintiff's and Class members' PI as part of its general course of business.

60. MIE knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. MIE also knew about numerous, well-publicized data breaches.

61. MIE knew, or should have known, that its computer systems did not adequately safeguard Plaintiff's and Class members' PI.

62. Because MIE knew that a breach of its systems would damage hundreds of thousands of individuals, including Plaintiff and Class members, it had a duty to adequately protect their PI.

63. MIE had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust MIE with their Personal Information was predicated on the understanding that MIE would take adequate security precautions. Moreover, only MIE had the ability to protect its systems and the Personal Information it stored on them from attack.

64. MIE also had independent duties under state laws that required MIE to reasonably safeguard Plaintiff's and Class members' PI and promptly notify them about the Security Breach.

65. MIE breached the duties it 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 PI both before and after learning of the Security Breach;

c. by failing to comply with the minimum industry data security standards during the period of the Security Breach; and

d. by failing to timely and accurately disclose that their PI had been improperly acquired or accessed.

66. But for MIE's wrongful and negligent breach of the duties it owed Plaintiff and Class members, their PI either would not have been compromised or they would have been able to prevent some or all of their damages.

67. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of MIE's negligent conduct. Accordingly, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Separate Statewide Breach of Implied Contract Classes)

68. Plaintiff realleges, as if fully set forth, each and every allegation herein.

69. When Plaintiff and the members of the Nationwide Class or, alternatively, the members of the separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their PI to MIE, they entered into implied contracts by which MIE agreed to protect their PI and timely notify them in the event of a data breach.

70. An implicit part of the agreement regarding MIE's use of PI was that MIE would safeguard the PI using reasonable or industry-standard means and would timely notify Plaintiff and the Class in the event of a data breach.

71. Based on the implicit understanding, Plaintiff and the Class provided MIE with their PI.

72. Plaintiff and Class members would not have provided their PI to MIE had they known that MIE would not safeguard their PI as promised or provide timely notice of a data breach.

73. Plaintiff and Class members fully performed their obligations under the implied contracts with MIE.

74. MIE breached the implied contracts by failing to safeguard Plaintiff's and Class members' PI and failing to provide them with timely and accurate notice when their PI was compromised in the Security Breach.

75. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of MIE's breaches of its implied contracts with them.

COUNT IV

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CALIFORNIA CIVIL CODE § 1798.81.5

(On Behalf of Plaintiff and the California Class)

76. Plaintiff realleges, as if fully set forth, each and every allegation herein.

77. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act, California Civil Code § 1798.81.5, which requires that any business that "owns licenses or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

78. As described above, MIE failed to implement and maintain reasonable security procedures and practices to protect the Plaintiff's and California Class members' PI, and thereby violated the California Customer Records Act.

79. By violating section 1798.81.5 of the California Customer Records Act, MIE is liable to Plaintiff and California Class members for damages under California Civil Code section 1798.84(b).

80. Because MIE "violates, proposes to violate, or has violated," the California Customer Records Act, Plaintiff is entitled to injunctive relief under California Civil Code section 1798.84(e).

81. Accordingly, Plaintiff requests that the court enter an injunction that requires MIE to implement reasonable security procedures and practices, including, but not limited to: (1) ordering that MIE engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on MIE's systems on a periodic basis, and ordering MIE to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that MIE engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that MIE audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that MIE segment data by, among other things, creating firewalls and access controls so that if one area of MIE is compromised, intruders cannot gain access to other portions of MIE's systems; (5) ordering that MIE purge, delete, and destroy in a reasonably secure manner data not necessary for its provisions of services; (6) ordering that MIE conduct regular database scanning and securing checks; (7) ordering that MIE 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 (8) ordering MIE to meaningfully educate its users about the threats they face as a result of the loss of their PI to third parties, as well as the steps MIE users must take to protect themselves.

///

///

///

///

COUNT V

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE § 56, *ET SEQ*.

(On Behalf of Plaintiff and the California Class)

82. Plaintiff realleges, as if fully set forth, each and every allegation herein.

83. California Civil Code § 56.10 provides that "[a]o provider of health care, health care service plan, or contract or shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining authorization."

84. At all relevant times, pursuant to California Civil Code § 56.06(a), MIE was both a contractor and a health care provider under California law because it had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of an individual or a provider of health care, for purposes of . . . diagnosis and treatment of the patient." In particular, MIE is a privately incorporated business that works to "share information throughout a complex healthcare community that includes hospitals, physicians, laboratories and diagnostic testing facilities and – of course – patients." Medical Informatics Engineering, http://www.mieweb.com/company/about.

85. At all relevant times, MIE collected, stored, managed and transmitted Plaintiff's and Class members' PI and made such information available to MIE's clients upon request.

86. California Civil Code § 56, *et seq*., requires MIE to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to it. Specifically, California Civil Code § 56.10(a) prohibits MIE

from disclosing Plaintiff's and Class members' PHI without first obtaining the appropriate authorization to do so.

87. California Civil Code § 56.11 specifies the manner by which authorization must be obtained by providers of health care before PHI is released. MIE failed to obtain proper authorization before releasing Plaintiff's and Class members' PHI and failed to adopt and maintain the requisite protective procedures required by California law. As a direct and/or proximate result of MIE's wrongful actions, inaction, and/or omissions, Plaintiff's and Class members' PHI was wrongfully disclosed to the world. As described in detail above, the wrongfully disclosed and compromised PHI was transferred, sold, opened, read, mined and otherwise used without Plaintiff's and Class members' authorization. By disclosing Plaintiff's and Class members' PHI in this manner without their written authorization and subjected their PHI to being transferred, sold, opened, read, mined and otherwise used without authorization, MIE violated California Civil Code § 56, *et seq*., and its legal duty to protect the confidentiality of such information.

88. MIE also violated sections 56.06 and 56.101 of the California Confidentiality of Medical Information Act, which prohibits the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential PHI. As a direct and/or proximate result of MIE's wrongful actions, inaction, and/or omissions that directly and/or proximately caused the Security Breach, Plaintiff's and Class members' confidential PHI was wrongfully released and disclosed.

89. As a direct and/or proximate result of MIE's wrongful actions, inaction, and/or omissions that directly and/or proximately caused the Security Breach, Plaintiff and Class members have suffered (and continue to suffer) economic damages and other injury and harm in the form of, *inter alia*; (i) actual identity theft, identity fraud and/or medical fraud; (ii) invasion of privacy;

(iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vi) diminished value of the healthcare products, medical insurance and/or medical services they purchased from MIE's clients; and/or (vii) an imminent, immediate and/or continuing increased risk of identity theft, identity fraud and/or medical fraud – for which they are entitled to compensation.

90. Pursuant to California Civil Code §§ 56.35 and 56.36(b)(1), Plaintiff and members of the California Class also are entitled to appropriate injunctive and declaratory relief against MIE, an award of statutory liquidated damages of $1,000 to Plaintiff and each California Class member, punitive damages of up to $3,000 for Plaintiff and each California Class member, attorneys' fees, litigation expenses and court costs.

COUNT VI

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, *ET SEQ*.

(On Behalf of Plaintiff and the California Class)

91. Plaintiff realleges, as if fully set forth, each and every allegation herein.

92. The California Unfair Competition Law, California Business & Professions Code § 17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By reason of the wrongful actions, inaction, and/or omissions alleged herein, MIE engaged in unlawful and unfair practices within the meaning of the UCL.

93. As a direct and/or proximate result of MIE's wrongful actions, inaction, and/or omissions that directly and/or proximately caused the Security Breach, Plaintiff and California Class members have suffered (and will continue

to suffer) economic damages and other injury and harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or medical fraud; (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI; (iv) statutory nominal damages of $,1000 per Plaintiff and each Class member under the California CMIA (Cal. Civ. Code § 56.36(b)(1)); (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages; and (vii) the imminent, immediate and continuing increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to compensation.

94. In the course of conducting business, MIE committed "unlawful" business practices by, *inter alia*, failing to provide and/or take reasonable security measures for the collection, storage and transmission of Plaintiff's and Class members' PII/PHI, violating the statutory and common law alleged herein, including the California Customer Records Act and California Confidentiality of Medical Information Act. Plaintiff and California Class members reserve the right to allege other violations of law that constitute other unlawful business acts or practices. Such conduct is ongoing and continues to this date.

95. MIE also violated the UCL by failing to immediately notify Plaintiff and Class members of the wrongful disclosure of their PII/PHI. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI, finances, and identities.

96. MIE's wrongful actions and/or inaction, omissions, misrepresentations, practices and non-disclosures as alleged herein also constitute "unfair" business acts and practices, within the meaning of Cal. Bus. & Prof. Code § 17200, *et seq*., in that MIE's conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive and unscrupulous, and the gravity of MIE's wrongful conduct outweighs any alleged

benefits attributable to such conduct. There were reasonably available alternatives to further MIE's legitimate business interests other than the wrongful conduct described herein.

97. MIE's wrongful actions, inaction, and/or omissions, and the resulting Security Breach, directly and/or proximately caused (and continues to cause) the above-described substantial economic damages and other injury and harm to Plaintiff and California Class members. Unless restrained and enjoined, MIE will continue to engage in the above-described wrongful conduct.

98. Plaintiff, on behalf of herself, California Class members and the general public, also seeks restitution, an injunction prohibiting MIE from continuing such wrongful conduct and requiring MIE to take further actions to protect Plaintiff's and Class members' PII/PHI, and all other relief this Court deems just, proper, and consistent with Cal. Bus. & Prof. Code § 17203.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes set forth herein, respectfully request that the Court enter judgment in their favor that:

A. certifies the Classes requested, appoints Plaintiff as class representatives of the applicable classes and her undersigned counsel as Class counsel;

B. awards Plaintiff and Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement,

C. on behalf of Plaintiff and the Statewide Classes, enters an injunction that requires MIE to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiff's PI, which remains in the possession of MIE;

D. on behalf of Plaintiff and the Statewide Data Breach Statute Classes, awards appropriate equitable relief, including an injunction requiring MIE to promptly notify all affected customers of future data breaches;

E. orders MIE to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

F. awards Plaintiff and the Classes pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

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

JURY TRIAL DEMANDED

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

Dated: August 6, 2015

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
PAULA M. ROACH (254142)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

701 B Street, Suite 1700
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
tblood@bholaw.com
toreardon@bholaw.com
proach@bholaw.com

FEDERMAN & SHERWOOD
WILLLIAM B. FEDERMAN *****
CARIN L. MARCUSSEN *****
10205 N. Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Tel: 405/235-1560
405/239-2112 (fax)
wbf@federmanlaw.com
clm@federmanlaw.com

***** Admission *pro hac vice* to be sought

Attornevs for Plaintiff