UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
SOUTH BEND DIVISION

In Re: Medical Informatics Engineering, Inc., Customer Data Security Breach Litigation (MDL 2667) This Document Relates to All Cases	Case No.: 3:15-MD-2667 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs identified below ("Plaintiffs"), individually, and on behalf of the Classes of similarly situated persons defined below, file this superseding Consolidated Amended Class Action Complaint pursuant to the Court's Case Management Order (Doc. No. 36) and the Court's Practice and Procedure Order Upon Transfer Pursuant to 28 U.S.C. § 1407(a) (Doc. No. 11). Plaintiffs file suit against Defendants Medical Informatics Engineering, Inc. and NoMoreClipboard, LLC ("Defendants").

INTRODUCTION

1. Between May 7, 2015 and May 26, 2015, hackers infiltrated and accessed the inadequately protected computer systems of Defendant Medical Informatics Engineering, Inc. ("MIE") and Defendant NoMoreClipboard, LLC ("NMC"). During that time, the hackers stole the protected personal information and protected health information of 3.9 million individuals ("Breach Victims") whose information was contained in an electronic medical record stored in Defendants' computer systems. The personal information obtained by the hackers

includes names, telephone numbers, mailing addresses, usernames, hashed passwords, security questions and answers, spousal information (names and potentially dates of birth), email addresses, dates of birth, and Social Security numbers ("Personal Information"). The protected medical information obtained by the hackers includes lab results, health insurance policy information, diagnosis, disability codes, doctors' names, medical conditions, and children's name and birth statistics ("Medical Information").

2. Defendants' conduct—failing to take adequate and reasonable measures to ensure their computer systems were protected, failing to take available steps to prevent and stop the breach, failing to disclose the material facts that they did not have adequate computer systems and security practices to safeguard Personal and Medical Information, failing to honor their repeated promises and representations to protect the Breach Victims' Personal and Medical Information, and failing to provide timely and adequate notice of the MIE data breach—has caused substantial harm and injuries to consumers across the United States.

3. As a result of the MIE data breach, Breach Victims have been harmed. For example, Breach Victims have had fraudulent charges on various accounts. They have spent many hours filing police reports and monitoring credit reports and credit and bank accounts to combat identity theft. Many are now paying monthly or annual fees for identity theft and credit monitoring services. Now that their Personal and Medical Information has been released, Breach Victims must be super-vigilant and worry about being victimized for the rest of their lives.

JURISDICTION & VENUE

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

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 based on the transfer order of the Judicial Panel on Multidistrict Litigation. Venue was proper in this Court with respect to the actions originally filed in this Court pursuant to 28 U.S.C. § 1391 because MIE is headquartered in this district and regularly transacts business in this district, and many Class members reside in this district. The causes of action for the class members also arose, in part, in this district.

PARTIES

I. Plaintiffs

Arkansas

6. Plaintiff, Antionette Ann Franklin, is a citizen of the State of Arkansas. Ms. Franklin received a letter from MIE informing her that her address, password, username, security question, phone, email address, and birth date were compromised as a result of the MIE data breach. The letter also informed Ms. Franklin that MIE received her information from MIE's client, Arkansas Otolaryngology, P.A. As a consequence of MIE's data breach, Ms. Franklin is

compelled to more closely monitor her credit and other accounts. Ms. Franklin spent tens of hours setting up fraud alerts that last for seven years with three credit bureaus, purchasing a background check with the Arkansas State Police that cost $27, seeking legal representation, filing a complaint with the Department of Homeland Security Office for Civil Rights, researching identity theft protection resources, and conducting an independent investigation of the MIE data breach. Ms. Franklin also began receiving suspicious emails after the MIE data breach.

Arizona

7. Plaintiff, Ira Kushner, is a citizen of the State of Arizona. Mr. Kushner received a letter from MIE informing him that his social security number, address, telephone number, and birth date were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Kushner is compelled to more closely monitor his credit and other accounts and spend numerous hours addressing issues arising from the MIE data breach.

California

8. Plaintiff Steve Walker is a citizen of the State of California. He received a letter from MIE stating that his social security number, birth date, address, phone number, and email address were compromised in the MIE data breach. After the MIE data breach, Mr. Walker received a suspicious phone call from a person with a strong foreign accent who knew the specific blood pressure medication he was taking and solicited Mr. Walker to purchase an alternative medication. His phone number is a cell phone number, which is an unlisted number.

Also, after the MIE breach, Mr. Walker began receiving phishing emails regarding health issues and solicitations for medications, some of which were specific to Mr. Walker's specific medical issues. As a consequence of the MIE breach, Mr. Walker is compelled to more closely monitor his financial and medical accounts, a time-consuming process.

Florida

9. Plaintiff, Allan Lewis, is a citizen of the State of Florida. Mr. Lewis received a letter from MIE informing him that his name, address, and social security number were compromised as a result of the MIE data breach. The letter also informed Mr. Lewis that MIE received his information from MIE's client, Concentra. As a consequence of MIE's data breach, Mr. Lewis is compelled to more closely monitor his credit and other accounts and sign up for the two year credit monitoring service offered by MIE through Experian. So far, Mr. Lewis has spent tens of hours investigating the data breach and monitoring his accounts. While monitoring these accounts, Mr. Lewis has so far noticed two incidents of fraudulent activity on his accounts: (1) a Sprint account was fraudulently opened in his name in June of 2015; (2) a Capital One account was fraudulently opened in his name in November of 2015.

Georgia

10. Plaintiff, David Wayne Perry, is a citizen of the State of Georgia. Mr. Perry received a letter from MIE informing him that his social security number was compromised as a result of the MIE data breach. As a consequence of MIE's

data breach, Mr. Perry is compelled to sign up for the two year credit monitoring service offered by MIE through Experian and spend time each month monitoring his credit and other accounts. Shortly after the MIE data breach, in July 2015, Mr. Perry began receiving suspicious emails requesting that he cash checks and share his address.

Indiana

11. Plaintiff James Young is a citizen of the State of Indiana. Mr. Young received a letter from MIE informing him that his address, phone number, date of birth, and clinical data were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Young is compelled to more closely monitor his credit and other accounts and spend time addressing issues arising from the MIE data breach.

12. Plaintiff, Cynthia Weinman, is a citizen of the State of Indiana. Mrs. Weinman received a letter from NoMoreClipboard informing her that her Personal Information was compromised as a result of the MIE data breach. The letter also informed Mrs. Weinman that NMC received her information from NMC's client, Parkview Hospital and its affiliated labs. As a consequence of MIE's data breach, Mrs. Weinman is compelled to more closely monitor her credit and other accounts. Since the MIE data breach, Mrs. Weinman's debit card has had fraudulent activity and was cancelled. As a result, she had to open a new card with PNC. As a result of the MIE data breach, Mrs. Weinman has spent and continues to spend numerous hours addressing issues arising from the MIE data breach.

13. Plaintiff, Patricia Justice, is a citizen of the State of Indiana. Ms. Justice received a letter from MIE informing her that her social security number, address, phone, email, birth date, and medical information were compromised as a result of the MIE data breach. The letter also informed Ms. Justice that MIE received her information from MIE's clients**,** Fort Wayne Radiology Association, LLC, Allied Physicians d/b/a Fort Wayne Neurological Center, Redi-Med, No More Clipboard, and Ear Nose and Throat Associates. As a consequence of MIE's data breach, Ms. Justice is compelled to more closely monitor her credit and other accounts and sign up for the two year credit monitoring service offered by MIE through Experian. Ms. Justice now spends time each day monitoring her credit and other accounts, as well as potential cyber intrusions to her computers, and checking her bank account for unauthorized charges. After the MIE data breach, she noticed unauthorized charges on a Capital One credit card account and a debit card connected with a checking account. She also received a letter turning her down for a loan she never applied for. As a result of the MIE data breach, Ms. Justice has started carrying cash and paying for things with cash, and she closed two bank accounts and, in order to avoid having to pay for things on-line, started requesting paper statements.

14. Plaintiff Thomas Jones is a citizen of the State of Indiana. Mr. Jones received a letter from MIE informing him that his social security number, address, phone, checking account, email, birth date, clinical data, and medical records were compromised as a result of the MIE data breach. The letter also informed Mr. Jones

that MIE received his information from at least eleven of MIE's clients, including Accustat Medical Lab, Inc. and Indiana Urgent Care Centers, LLC. As a consequence of MIE's data breach, Mr. Jones is compelled to purchase a shredder and shred documents consistently and peel the labels off prescription medicine containers before disposing of them. Mr. Jones also no longer purchases items on the internet; instead, he uses either cash or a pre-paid debit card that is not linked to his bank account. Since the breach, he and his wife no longer pay for things using personal checks and they retained a financial advisor, who sends him a copy of his credit reports once a month. In June 2015, unauthorized purchases were made on Mr. Jones's bank debit card, which caused his checking account to have insufficient funds to pay recurring automated bills. The bank charged him overdraft fees, which were ultimately refunded, but he had to pay approximately $400 in late or overdraft charges to his creditors. Mr. Jones spent time each week talking to the bank and his creditors trying to get these problems fixed. In November 2015, Mr. Jones went to the local state police and paid $24 to run a search using his social security number.

Kansas

15. Plaintiff Herbert L. Schuttler is a citizen of the Commonwealth of Kansas. Mr. Schuttler received a letter from MIE informing him that his social security number, address, phone, and birth date were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Schuttler is compelled to spend time scrutinizing all financial, account, and credit information and sign up for the two year credit monitoring service that MIE offered through

Experian. Since MIE's data breach, he has received suspicious emails. As a result of MIE's data breach, Mr. Schuttler has observed a questionable credit card charge that is under investigation.

Kentucky

16. Plaintiff Jeremy Brann is a citizen of Kentucky. He received a letter from MIE stating that his social security number, birth date, home address, and email address were compromised in the MIE data breach. After the MIE data breach, on July 10, 2015, an unauthorized person obtained enough personal information about Mr. Brann to call his bank, pose as him, obtain access to his checking and savings accounts, transfer funds from his savings account to his checking account, increase the withdrawal limit, and withdraw over $5,000 from an ATM machine in Dubai. The bank later informed Mr. Brann that it asked the thief six security questions, and the thief answered five of them correctly, which was enough to gain access to the account. The questions answered correctly involved many of the same data points as those compromised in the MIE data breach, including Mr. Brann's social security number, birth date, address, name, and the social security number of his wife (she was affected by the MIE breach and received a separate breach letter from MIE). Subsequently, the bank placed Mr. Brann's account on a watch list. Thereafter, while traveling in London, Mr. Brann tried to withdraw cash from an ATM machine, but the bank denied the withdrawal because it was deemed suspicious. The bank then had to send a code to Mr. Brann's phone and ask a series of detailed questions to verify his identity. Mr. Brann spent hours

on the phone with the bank, and incurred charges for overages in cell minutes and data usage. As a consequence of the MIE breach, he also placed a credit freeze on his credit report, which is an ongoing inconvenience because it restricts his access to credit.

Louisiana

17. Plaintiff, Cynthia Benoit, is a citizen of the State of Louisiana. Ms. Benoit received a letter from MIE informing her that her social security number, address, email address, and birth date were compromised as a result of the MIE data breach. The letter also informed her that MIE received this information from MIE's client, Concentra. As a consequence of MIE's data breach, Ms. Benoit is compelled to more closely monitor her credit and other accounts and sign up for the two year credit monitoring service offered by MIE through Experian. Additionally, she ordered and reviewed her credit reports. As a consequence of MIE's data breach, Ms. Benoit checks her accounts daily and changes her passwords every three months and had to file a police report.

Michigan

18. Plaintiff Floyd Harris is a citizen of Michigan. He received a letter from MIE stating that his social security number, address, phone number, email address, birth date, username, password, and security question were compromised in the MIE data breach. After the MIE breach, Mr. Harris received unsolicited phone calls and emails seeking to sell him medication and medical equipment. In certain instances, the callers or senders of the emails knew his specific medical

conditions. Also, after the breach, Mr. Harris began receiving unsolicited letters and emails seeking his participation in medical studies for his specific medical conditions. Further, after the breach, he noticed an increase in phishing emails requesting his personal and financial information. As a consequence of the breach, he is compelled to more closely monitor his financial and medical accounts, which is a time-consuming process.

Nevada

19. Plaintiff, Lauren Fern Rainess, is a citizen of the State of Nevada. Ms. Rainess received a letter from MIE informing her that her social security number, address, and date of birth were compromised as a result of the MIE data breach. The letter also informed Ms. Rainess that MIE received her information from MIE's client, Concentra. As a consequence of MIE's data breach, Ms. Rainess made multiple calls to the three credit bureaus to review the status of her credit, reviewed and removed fraudulent credit inquiries on her credit reports, froze her credit, and placed fraud alerts on her credit cards. She also filed two police reports, mailed letters to the credit agencies in California, and made multiple calls and two forty minute round trips to the police department. Ms. Rainess spent tens of hours completing these tasks.

New Jersey

20. Plaintiff, Anita Colter, is a citizen of the State of New Jersey. Ms. Colter received a letter from MIE informing her that her social security number, address, phone, and birth date were compromised as a result of the MIE data

breach. The letter also informed Ms. Colter that MIE received her information from MIE's client, Concentra. Prior to the MIE data breach, she was a subscriber to a credit monitoring service called Legal Shield, which monitors her accounts for potential fraud. As a consequence of MIE's data breach, Ms. Colter is compelled to sign up for the two year credit monitoring service offered by MIE through Experian and report the MIE data breach to her banks and credit card providers. Additionally, Ms. Colter ordered copies of her credit report shortly after receiving MIE's letter. Ms. Colter is now relying upon Experian's credit monitoring service and the Legal Shield service for which she continues to pay.

New Mexico

21. Plaintiff, Richard Larson, is a citizen of the State of New Mexico. Mr. Larson received a letter from MIE informing him that his social security number, address, email, and date of birth were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Larson is compelled to more closely monitor his credit and other accounts and sign up for the two year credit monitoring service offered by MIE through Experian and spend numerous hours addressing issues arising from the MIE data breach.

Ohio

22. Plaintiff Michael Osbourn is a citizen of the State of Ohio. Mr. Osbourn received a letter from MIE informing him that his social security number, address, phone number, birth date, and clinical data were compromised as a result of the MIE data breach. The letter also informed Mr. Osbourn that MIE received his

information from MIE's clients, Fort Wayne Radiology, Allied Physician, and B.B.A. Fort Wayne Neurological Center. As a consequence of MIE's data breach, Mr. Osbourn is compelled to more closely monitor his credit and other accounts, sign up for the two year credit monitoring service offered by MIE through Experian, and spend numerous hours addressing issues arising from the MIE data breach. While monitoring these accounts after the MIE data breach, Mr. Osbourn noticed he began receiving suspicious emails.

Oregon

23. Plaintiff Mark Guth is a citizen of the State of Oregon. Mr. Guth received a letter from MIE informing him that his name, address, and social security number were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Guth is compelled to more closely monitor his credit and other accounts sign up for the two year credit monitoring service offered by MIE through Experian. Additionally, Mr. Guth purchased MyFico.com for $29.95 per month and also placed fraud alerts on his credit cards and ordered and reviewed his credit reports. He also changes his passwords every three months, checks his credit reports through his Discover card, and monitors his credit daily. After the MIE data breach, Mr. Guth noticed he began receiving suspicious emails.

Pennsylvania

24. Plaintiff Richard DiGovine is a citizen of the Commonwealth of Pennsylvania. Mr. DiGovine received a letter from MIE informing him that his name, address, social security number, birth date, and email address were

compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. DiGovine is compelled to more closely monitor his credit and other accounts, order and review his credit reports, spend time reviewing these credit reports, spend money purchasing a supplemental credit report, and sign up for the two-year credit monitoring service offered by MIE through Experian. Mr. DiGovine now checks his financial statements, at least weekly, checks his Experian credit monitoring account monthly, and receives reports from Experian.

Texas

25. Plaintiff, Brandon Warrick, is a citizen of the State of Texas. Mr. Warrick received a letter from MIE informing him that his Personal Information was compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Warrick is compelled to more closely monitor his credit and other accounts and spend numerous hours addressing issues arising from the MIE data breach.

Virginia

26. Plaintiff James Mueller is a citizen of the Commonwealth of Virginia. Mr. Mueller received a letter from MIE informing him that his address and birth date were compromised as a result of the MIE data breach. As a consequence of MIE's data breach, Mr. Mueller is compelled to more closely monitor his credit and other accounts and sign up for the two year credit monitoring service offered by MIE through Experian. Additionally, Mr. Mueller ordered and reviewed his credit reports and spent time reviewing these reports and routinely checks his credit

reports, monitors his bank and credit card statements, and changes his passwords every ninety days. After the data breach, Mr. Mueller noticed he began receiving suspicious emails.

Washington

27. Plaintiff Michelle Moore is a citizen of the State of Washington. Ms. Moore received a letter from MIE informing her that her social security number, address, phone, email, and birth date were compromised as a result of the MIE data breach. The letter also informed Ms. Moore that MIE received her information from MIE's client, Concentra. As a consequence of MIE's data breach, Ms. Moore is compelled to more closely monitor her credit and other accounts and sign up for the credit monitoring service offered by MIE through Experian, as well as another program through her bank. She has also monitored her credit through Credit Karma. Ms. Moore spent a significant amount of time setting up these credit monitoring services, and checks her credit at least twice per week. While monitoring these accounts after the MIE data breach, Ms. Moore noticed she began receiving suspicious emails.

II. Defendants

28. Defendant MIE is a citizen of the State of Indiana. MIE is a corporation that is incorporated in Indiana and has its principal place of business in Indiana at 6302 Constitution Drive, Fort Wayne, IN 46804.

29. Defendant NoMoreClipboard, LLC ("NMC") is a citizen of the State of Indiana because it is a wholly-owned subsidiary of MIE, thus all of its member(s)

are citizens of Indiana. NMC is organized in Indiana and has its principal place of business in Indiana at 6312 Constitution Drive, Fort Wayne, IN 46804.

30. NMC is a wholly-owned subsidiary of MIE and shares founders, officers, employees, offices, and servers with MIE.

31. Prior to January 6, 2016, MIE also operated under the assumed name of Enterprise Health and/or Enterprise Health was a division of MIE. On January 6, 2016, MIE formed Enterprise Health, LLC, which shares founders, officers, employees, offices, and servers with MIE and NMC.

32. K&L Holdings, LLC is affiliated with MIE and has the same founders, officers, and offices as MIE, NMC, and Enterprise Health. K&L Holdings, LLC owns the property that serves as the headquarters for K&L Holdings, LLC, MIE, NMC, and Enterprise Health.

STATEMENT OF FACTS

III. MIE's Computer Systems

33. MIE was founded in 1995 by Eric Jones and Doug Horner.

34. As a "leading innovator" in the health information technology field, MIE hosts on its servers electronic medical records ("EMR") that can be shared electronically between health care providers through networks called health information exchanges ("EMR Services").

35. MIE's wholly owned subsidiary, NMC, was founded in 2005 by Eric Jones and Doug Horner and provides substantially the same services as MIE except that its services are directed towards consumers and employers.

36. NMC uses MIE's computer systems and servers.

37. Defendants' clients ("Clients") include employers that operate on-site employee health clinics, such as Google and Eli Lilly, and health care providers, such as Concentra and Franciscan St. Francis Health Indianapolis, and consumers.

38. As of March 2011, Defendants hosted 7 million patient charts and 13.2 million diagnostic images on its servers. (*Changing Industry Spurs MIE's Growth*, Great Fort Wayne Business Weekly, Mar. 18, 2011.) At that time, Defendants' Clients included 65% of physicians in the northern Indiana region. (*Id.*)

39. Defendants' Clients can access the EMR Records hosted on Defendants' servers through a log-in on a web browser on a personal computer, iPad, iPhone, or Smartphone.

40. The EMR records "at rest" on Defendants' servers are not encrypted. Data "at rest" means data stored physically in any digital form, such as databases, data warehouses, spreadsheets, archives, tapes, off-site backups, and mobile devices.

41. Defendants enter into standard form agreements (the "Agreement") with their Clients under which the Client pays MIE, starting at $250 per physician per month, for monthly charges for MIE's EMR services. An example of Defendants' Agreement with their Clients is attached as Exhibit "A."

42. Defendants' Clients also pay a one-time licensing fee for access to MIE's licensed software, which can cost nearly $50,000.

43. Defendants' Clients also pay MIE an annual maintenance fee.

IV. Defendants Promised to Protect Personal and Medical Information

44. Defendants made promises to protect Plaintiffs' and Class Members' Personal and Medical Information.

45. Defendants' Agreements with their Clients contain a promise by Defendants to "keep confidential and not disclose any . . . Confidential Information . . . to which MIE is permitted access or which is disclosed to MIE . . . ." (Ex. A at 9, ¶ 8.9(b); *see also* Ex. B at ¶ 10.1 ("MIE . . . acknowledge[s] . . . all material and information of the other party which has or will come into its possession or knowledge in connection with this Agreement or its performance, consists of confidential . . . information . . . whose unauthorized disclosure to or use by third parties may cause immediate and irreparable harm to the other party. Both parties therefore agree to hold the Confidential Information of the other party in the strictest confidence . . . and not to release or make any portion of it available . . . for copying or use by any third party.").)

46. Uniformly, those Agreements also provide that they are governed by the laws of the State of Indiana, without reference to its choice of law rules, and that venue for litigation regarding any aspect of the Agreement will be located in Allen County, Indiana, or the United States Federal Courts for the Northern District of Indiana. (Ex. A. at 8, ¶ 8.1; Ex. B. at ¶ 33.)

47. Effective December 1, 2011, MIE's website made promises to follow the law:

Privacy Policy Statement

MIE strives to collect, use, and disclose personal information associated with its EMR product ("EMR Data") in a manner consistent with applicable laws as well as the requirements of its clients. MIE upholds a tradition of the highest ethical standards in its business practices. MIE is a "Business Associate" pursuant to the Health Insurance Portability and Accountability Act and its Privacy Rule and Security Rule provisions (collectively, "HIPAA") for many of its clients whose use of the EMRs are considered "Covered Entity" functions under HIPAA. As a HIPAA Business Associate with respect to the handling of the EMR Data of clients, MIE adheres to all HIPAA requirements, including the enhancements introduced by the HITECH Act of 2009, and its handling of the EMR Data is undertaken only as specified in the business associate agreements with its clients.

With respect to the receipt and processing of EMR Data from clients when the EMR Data originates in the EU/EEA, MIE hereby certifies that it adheres to the U.S./E.U. Safe Harbor Frameworks (i.e., Privacy Principles and the fifteen "Frequently Asked Questions"; hereinafter, collectively, the "Privacy Principles") as set forth by the U.S. Department of Commerce. MIE specifically certifies that it adheres to the relevant Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement in fulfilling its relevant contractual responsibilities assigned by the client for the receipt, processing, storage, and reporting of EMR Data as received from its clients. This Safe Harbor Privacy Policy does not apply to information or data other than the EMR Data from the EU/EEA that it receives from its clients.

. . .

Any questions, concerns, or complaints regarding the use or disclosure of personal information should be directed to the MIE Privacy Officer at the address given below. Any MIE employee who receives a question, concern, or complaint regarding the use or disclosure of personal information will direct that information to MIE's Privacy Officer. MIE will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this Policy. . . .

(*Medical Informatics Engineering, Inc.—Safe Harbor Privacy Policy*, http://www.mieweb.com/company/certifications/safeharbor (last visited Feb. 12, 2016).)

48. Effective February 18, 2010, MIE's website also made promises regarding its privacy policies:

> **Privacy Policy**
>
> At Medical Informatics Engineering (MIE), protecting your privacy is of the utmost importance. Information furnished by you to us will be treated with the greatest respect . . . In this policy, "personal information" refers to names, home and office contact information and any other "information relating to an identified or identifiable natural person."
>
> . . . This privacy policy applies collectively to MIE's security practices and to all data collected by, used by or exchanged among any of the MIE's legal entities. . . .
>
> HOW IS YOUR INFORMATION SECURED AND PROTECTED?
>
> Medical Informatics Engineering uses encryption and authentication tools (password and user identification) to protect your personal information. However, emails sent via the Site may not be secure during transmission. If your communication is very sensitive, or includes highly confidential information such as a credit card number or premium or loss information, you may want to send it by regular mail or verify that encryption is used.
>
> Our employees are aware that certain information provided by our customers is confidential and is to be protected. Employees who misuse customer information are subject to disciplinary action.
>
> . . .

(*Privacy Policy*, http://www.mieweb.com/privacy (last visited Feb. 12, 2016).)

49. NMC's website made promises regarding its privacy policies:

Privacy Policy

Health Insurance Portability and Accountability Act (HIPAA)

> Consumers are becoming increasingly aware of the need for privacy and security when storing personal information online. When it comes to healthcare, the situation is no different. At a national level, the healthcare industry is moving toward electronic storage of medical records. As this situation progresses, laws have been enacted to honor the privileged nature of information exchanged between patients and their doctors. HIPAA, the guiding rule of law on patient privacy, asserts that safeguards must be in place for "protected health information", defined by that same law as "individually identifiable information." (45 CFR 160.103)
>
> NoMoreClipboard.com was designed to support the privacy and security requirements of HIPAA while enabling you to use the service from any computer with Internet access. This service allows you to store, change, and direct your information to healthcare providers, as well as generate a report showing to whom you have sent your information. As it pertains to NoMoreClipboard.com, our responsibilities are to make the information you provide on our site available to you, and to administer the system to ensure that your privacy and security are protected.
>
> . . .
>
> NoMoreClipboard.com will not send your information to anyone without you directing it and/or consenting to it. . . .
>
> . . .
>
> All employees and agents of NoMoreClipboard.com are bound by a confidentiality agreement which prohibits the access and use of data for any other purpose than to assist NoMoreClipboard.com members.

(*Privacy Policy*, https://nomoreclipboard.com/nmc.cgi?f=layoutnouser&name=Privacy&wizard=2&mode=4 (last visited Feb. 22, 2016).) NMC's website also provides that any disputes regarding its services "will be governed by Indiana law for all purposes . . . without regard to or application of choice of law rules or

principles" and that venue is with the courts of Indiana. (*Terms of Use*, https://nomoreclipboard.com/nmc.cgi?f=layoutnouser&name=Terms+Page&wizard=2&mode=4 (last visited Feb. 22, 2016).)

V. Defendants Had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

50. Defendants admit that they are a "business associate" covered by HIPAA, *Medical Informatics Engineering, Inc.—Safe Harbor Privacy Policy*, http://www.mieweb.com/company/certifications/safeharbor (last visited Feb. 10, 2016), and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part 160 and Part 164.

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

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

53. Defendants admit the HITECH Act of 2009 applies to them. (*Medical Informatics Engineering, Inc.—Safe Harbor Privacy Policy*, http://www.mieweb.com/company/certifications/safeharbor (last visited Feb. 10, 2016).) That act expands the responsibilities of "business associates" under HIPAA's Privacy and Security Rules.

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

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

56. HIPAA's Security Rule requires Defendants to do the following:

1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the . . . business associate creates, receives, maintains, or transmits.

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted . . . .

4) Ensure compliance . . . by its workforce.

45 C.F.R. § 164.306(a).

57. HIPAA also requires Defendants 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).

58. HIPAA also requires Defendants 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).

59. Defendants are 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).

60. As described below, Defendants are also required by various state laws and regulations to protect Plaintiffs' and Class Members' Personal and Medical Information.

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

62. Defendants owed a duty to Breach Victims, whose Personal and Medical Information was entrusted to Defendants, to design, maintain, and test

their computer systems to ensure that the Personal and Medical Information in Defendants' possession was adequately secured and protected.

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

64. Defendants owed a duty to Breach Victims, whose Personal and Medical Information was entrusted to Defendants, to implement processes that would detect a breach on their data security systems in a timely manner.

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

66. Defendants owed a duty to Breach Victims, whose Personal and Medical Information was entrusted to Defendants, to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendants.

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

68. Defendants owed a duty of care to Breach Victims because they were foreseeable and probable victims of any inadequate data security practices. Defendants collected Breach Victims' Personal and Medical Information directly from those individuals and/or indirectly from individuals through MIE's Clients. Defendants knew that a breach of its data systems would cause Breach Victims to incur damages.

VI. Defendants Were on Notice of Cyber Attack Threats, and the Inadequacy of Their Data Security

69. Defendants knew or should have known about the inadequacy of their data security based on a prior breach of their systems.

70. In 2006, hackers infiltrated the software that MIE uses to provide EMR services to its Clients. (*FBI probes hacking incident at Indiana clinic*, Computerworld, Feb. 10, 2006.)

71. In early 2006, one of Defendants' clients began experiencing serious performance issues with MIE's software, which were caused by database changes made by someone who illegally accessed the software nine times over a period of two weeks that completely bypassed the front-end authentication. (*Id.*)

72. The FBI investigated the incident and Defendants publicly admitted to cooperating with that investigation. (*Id.*)

73. The Client that was the subject of that hack stopped using MIE's EMR Services as a result of that hack. (*Id.*)

74. Defendants were also on notice that companies in the healthcare industry were targets for cyberattacks.

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

76. Defendants were on notice that the federal government was concerned about healthcare company data encryption and Defendants knew they did not encrypt data "at rest." The United States Department of Health and Human Services' Office for Civil Rights urges the encryption of data containing sensitive personal information. In April 2014, the Department fined Concentra Health Services and QCA Health Plan Inc. of Arkansas 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 "[our] message to these

organizations is simple: encryption is your best defense against these incidents." (*Stolen laptops lead to important HIPAA settlements*, http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html# (last visited Feb. 22, 2016).)

VII. Defendants Allowed a Massive Data Breach

77. On June 10, 2015, MIE announced a "data security compromise that has affected the security of some personal and protected health information relating to certain clients and individuals who have used a Medical Informatics Engineering electronic health record." (http://www.mieweb.com/notice/ (last visited July 29, 2015).)

78. That same day NMC announced "a data security compromise that has affected the security of some personal and protected health information relating to individuals who have used a NoMoreClipboard personal health record or patient portal." (https://www.nomoreclipboard.com/notice (last visited Feb. 22, 2016).)

79. Defendants admitted that unauthorized access to their network began on May 7, 2015, but they did not discover suspicious activity until May 26, 2015.

80. Defendants then "began an investigation to identify and remediate any identified security vulnerability," hired "a team of third-party experts to investigate the attack and enhance data security and protection," and "reported this incident to law enforcement including the FBI Cyber Squad." (http://www.mieweb.com/notice/ (last visited July 29, 2015); https://www.nomoreclipboard.com/notice (last visited Feb. 22, 2016).)

81. Defendants also announced that that they were now going to "enhance the security of [their] systems" by: (i) "removing the capabilities used by the intruder to gain unauthorized access to the affected systems," (ii) "enhancing and strengthening password rules and storage mechanisms," (iii) "increase[ing] active monitoring of the affected systems," (iv) "intelligence exchange with law enforcement," and (v) "institut[ing] a universal password reset." (*Id.*)

82. MIE admitted that the following information was accessed by the hackers: "an individual's name, telephone number, mailing address, username, hashed password, security question and answer, spousal information (name and potentially date of birth), email address, date of birth, Social Security number, lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics." (http://www.mieweb.com/notice/ (last visited July 29, 2015).)

83. NMC admitted that the following information was accessed by the hackers: "an individuals' [sic] name, home address, Social Security number, username, hashed password, spousal information (name and potentially date of birth), security question and answer, email address, date of birth, health information, and health insurance policy information." (https://www.nomoreclipboard.com/notice (last visited Feb. 22, 2016).)

84. Defendants did not start mailing notification to Breach Victims until July 17, 2015, more than 2 months after the breach began on May 7.

85. Plaintiffs' and Class Members' stolen information was given to MIE by the following healthcare providers that are MIE's Clients:

- Concentra
- Allied Physicians, Inc. d/b/a Fort Wayne Neurological Center (including Neurology, Physical Medicine and Neurosurgery)
- Franciscan St. Francis Health Indianapolis
- Gynecology Center, Inc. Fort Wayne
- Rochester Medical Group
- RediMed
- Fort Wayne Radiology Association, LLC including d/b/a Nuvena Vein Center and Dexa Diagnostics
- Open View MRI, LLC
- Breast Diagnostic Center, LLC
- P.E.T. Imaging Services, LLC
- MRI Center — Fort Wayne Radiology, Inc. (f/k/a Advanced Imaging Systems, Inc.)

86. Further, individuals who received services from Fort Wayne Radiology Association, Open View, Breast Diagnostic Center, PET Imaging or MRI Center during the period of time from January 1, 1997 to May 26, 2015 were affected because the database relating to those healthcare providers was accessed on May 26, 2015.

87. MIE also admitted that victims may include, along with potential others, individuals who received radiology services during this time at any of the organizations identified below:

Accustat Medical Lab, Inc.	Indianapolis, IN
Allergy & Asthma Center	Fort Wayne, IN
Associated Physicians & Surgeons Clinic, LLC	Terre Haute, IN
Ball Memorial Hospital	Muncie, IN
Bedford Regional Medical Center	Bedford, IN
Cameron Memorial Community Hospital	Angola, IN
Central Indiana Orthopedics, PC	Muncie, IN
Community Memorial Hospital	Hicksville, OH
Ear, Nose & Throat Associates	Fort Wayne, IN
Family Medicine Associates, Jerry Sell, M.D.	Rockford, OH
First Care Family Physicians	Fort Wayne, IN
Fort Wayne Medical Oncology & Hematology	Fort Wayne, IN
Gary Pitts, M.D.	Warsaw, IN
Indiana Urgent Care Centers, LLC	Indianapolis, IN
Indiana University Health Center	Bloomington, IN
Jasper County Hospital	Rensselaer, IN
Manchester Family Physicians	North Manchester, IN
MedCorp	Toledo, OH
Meridian Health Group	Carmel, IN
Nationwide Mobile Imaging	Fort Wayne, IN
Neighborhood Health Clinic	Fort Wayne, IN
Orthopaedics Northeast	Fort Wayne, IN
Parkview Regional Medical Center	Fort Wayne, IN
Parkview Hospital	Fort Wayne, IN
Parkview Ortho Hospital	Fort Wayne, IN
Parkview Heart Institute	Fort Wayne, IN
Parkview Women & Children's Hospital	Fort Wayne, IN
Parkview Noble Hospital	Kendallville, IN
Parkview Huntington Hospital	Huntington, IN
Parkview Whitley Hospital	Columbia City, IN

Parkview LaGrange Hospital	LaGrange, IN
Parkview Physicians Group	
Parkview Occupational Health Centers	
Paulding County Hospital	Paulding, OH
Prompt Care Express	Coldwater, MI; Sturgis, MI
Public Safety Medical Services	Indianapolis, IN
Purdue University Health Center	W. Lafayette, IN
Southwestern Medical Clinics	Berrien Springs, MI
Tri-State Medical Imaging	Angola, Indiana
Union Associated Physicians Clinic	Terre Haute, IN
U.S. Healthworks Medical Group of Indiana	Elkhart, IN
Van Wert County Hospital	Van Wert, OH
Wabash County Hospital	Wabash, IN
Wabash Family Care	Wabash, IN

88. Plaintiffs' and Class Members' stolen information was given to NMC by over 200 physician practices, hospitals, and other employer organizations that are NMC's Clients. (https://www.nomoreclipboard.com/notice (last visited Feb. 22, 2016).)

89. Based on MIE's prior hack and public admissions about the MIE data breach, Defendants failed to implement basic industry-accepted data security tools to prevent cyberattacks from accessing MIE's systems: (1) Defendants did not implement a multi-factor authentication procedure for users to enter their computer system, instead allowing users to access MIE's servers from external systems using only a username and password. Conversely, in a multi-factor system, a user first enters his or her password, and then the user is sent a one-time second password (the second factor) to a personal device. The user receives a different second

password every time that the user signs on to his or her account. Multi-factor authentication has been a security best practice for remotely accessible systems for decades. (2) Defendants did not have sufficient password rules or storage mechanisms. If Defendants had implemented any of these basic data security tools, the cyber-attackers would not have been able to access Plaintiffs' and Class Members' Personal and Medical Information, or would not have been able to access so much of that information.

90. Defendants failed to implement sufficient monitoring and alerting that would have alerted them to the cyberattack during the weeks that the attack was ongoing. Defendants could have and should have, but failed to, discover the data breach before any data was stolen.

91. Defendants failed to encrypt the sensitive Personal and Medical Information within MIE's computer systems. If Defendants had encrypted that information, then even if the cyberattackers accessed MIE's computer systems, the cyberattackers would have been unable to use the Personal and Medical Information.

92. Defendants' publicly-admitted remedial measures—removing capabilities used to access the systems, enhancing and strengthening password rules and storage mechanisms, and increased active monitoring of the system—demonstrate inadequate aspects of their computer systems and data security practices, as these are all measures that should have been in place before the MIE data breach.

93. The remediation measures implemented by MIE provide only an immediate stop to the present attack and do not indicate that Defendants have made any changes to the policies, procedures, management methods, or practices that allowed these attacks to occur in the first place. New Personal and Medical Information is likely being entered into MIE's computer systems and this information is at risk until Defendants improve their data security.

VIII. Defendants' Data Breach Was a Direct Result of Their Inadequate Data Security

94. Plaintiffs' and Class Members' Personal and Medical Information was compromised in the MIE data breach because Defendants violated their promises and legal obligations to maintain the security of the highly sensitive Personal and Medical Information entrusted to Defendants.

95. Despite their promises and legal obligations, Defendants did not provide reasonable or adequate security for Plaintiffs' and Class Members' Personal and Medical Information. As the creator and main operator of its computer systems, MIE is responsible for the inadequate and unreasonable computer systems and data security practices.

96. Despite their promises and legal obligations, Defendants operated and maintained the deficient computer systems and data security practices.

97. Defendants breached their duty to Plaintiffs and Class Members to design, maintain, and test their computer systems to ensure that information was adequately secured.

98. Defendants breached their duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedure to protect Personal and Medical Information in their possession.

99. Defendants breached their duty to Plaintiffs and Class Members to implement processes that would detect a breach of their computer systems in a timely manner.

100. Defendants breached their duty to Plaintiffs and Class Members to disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard their Personal and Medical Information. Had Defendants disclosed to Plaintiffs and Class Members that their computer systems and data security practices were inadequate to safeguard Personal and Medical Information, Plaintiffs and Class Members would not have allowed their Personal and Medical Information to be entrusted to Defendants.

101. Defendants breached their duty to Plaintiffs and Class Members to disclose in a timely and accurate manner that the MIE data breach had occurred. Defendants failed to notify potentially affected customers for two months after they claim they discovered the breach. As a result, Plaintiffs and Class Members were not notified of the MIE data breach until July 2015 or later.

102. Defendants' failure to notify Plaintiffs and Class Members of the MIE data breach in a timely and accurate manner allowed the cyberattackers to begin to use the Personal and Medical Information before Plaintiffs and Class Members had an opportunity to take steps to protect themselves.

103. Defendants violated their promises contained in Agreements with their Clients that were intended to directly benefit Plaintiffs and Class Members.

104. Defendants violated their promise to "keep confidential and not disclose" Plaintiffs' and Class Members' Personal and Medical Information.

105. Defendants violated their promise to "hold . . . in strictest confidence . . . and not to release or make any portion [of Plaintiffs' and Class Members' Personal and Medical Information] available."

106. Defendants violated their promises and representations contained in their website privacy statements.

107. Defendants violated their promise to "protect [Plaintiffs' and Class Members'] personal information."

108. Defendants violated their promise to "ensure that [Plaintiffs' and Class Members'] privacy and security are protected."

109. Defendants violated their promise to "not send [Plaintiffs' and Class Members'] information to anyone without you directing it and/or consenting to it."

110. Defendants violated their promise to comply with federal and state law to maintain the security of Plaintiffs' and Class Members' Personal and Medical Information, such as HIPAA. For example, Defendants violated HIPAA by failing to establish procedures to keep Plaintiffs' and Class Members' Personal and Medical Information confidential and private.

111. Defendants violated the Federal Trade Commission Act by engaging in the "unfair practice" of failing to maintain reasonable and appropriate data security for consumers' Personal and Medical Information.

IX. Plaintiffs and Class Members Were Harmed by the MIE Data Breach

112. MIE's website provides "[f]raud prevention tips" that show just how harmful the MIE data breach is to Plaintiffs and Class Members. MIE "suggest[s] Breach Victims remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements for suspicious activity." MIE encourages Plaintiffs and Class Members "to notify their credit card companies, health care providers, and heath care insurers of this data security incident." MIE also instructs Plaintiffs and Class Members to "review explanation of benefits statement(s) that they receive from their healthcare provider or health plan," and if Plaintiffs or Class Members "see[ ] any service that he/she believes he/she did not receive, the individual should contact his/her health care provider or health plan at the telephone number listed on the explanation of benefits statement(s)." MIE also "suggest[s] that Breach Victims carefully review their credit reports," and "have the[ ] credit bureaus place a 'fraud alert' on their file that alerts creditors to take additional steps to verify his/her identity prior to granting credit in his/her name." (http://www.mieweb.com/notice/.)

113. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013). 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.*

114. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit. (*Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (September 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Feb. 24, 2016).

115. With access to an individual's Personal Information, criminals can commit various types of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

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

117. 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. *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), http://news.cnet.com/8301-27080_3-10460902-245.html. Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all. *Id*.

118. The injuries suffered by the Plaintiffs and Class Members are a direct and proximate result of the MIE data breach and include:

1) theft of their personal, medical, and financial information;
2) costs associated with the detection and prevention of identity theft and unauthorized use of their Personal and Medical Information and financial, business, banking, insurance, and other accounts;
3) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the MIE data breach, including finding fraudulent financial and medical charges, cancelling

credit cards, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, monitoring Explanations of Benefits, and the stress, nuisance, and annoyance of dealing with all issues resulting from the MIE data breach, including additional phishing emails and phone scams;

4) the imminent and certain impending injury flowing from fraud and identify theft posed by their Personal and Medical Information being placed in the hands of hackers;

5) damages to and diminution in value of their Personal and Medical Information entrusted to Defendants;

6) money paid to Defendants' Clients that was then paid to Defendants for health care services because Plaintiffs and Class Members would not have obtained health care services from Defendants' Clients had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' Personal and Medical Information;

7) overpayments to Defendants for health care services purchased from Defendants' Clients, in that a portion of the price paid by Plaintiffs and Class Members to Defendants' Clients was for the costs for Defendants to take reasonable and adequate security measures to protect

Plaintiffs' and Class Members' Personal and Medical Information, which Defendants failed to do;

8) damages caused by Defendants' failure to notify Plaintiffs and Class Members about the MIE data breach in a timely and accurate fashion; and

9) continued risk to Plaintiffs' and Class Members' Personal and Medical Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the that information entrusted to Defendants.

119. Defendants themselves acknowledge the harm caused by the data breach because they offered Plaintiffs and Class Members twenty-four months of identity theft repair and credit monitoring services. Two years of identity theft repair and credit 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.

CLASS ACTION ALLEGATIONS

120. Plaintiffs bring 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) are met with respect to the Class defined below.

121. The Plaintiff Class consists of all persons whose Personal or Medical Information was compromised by the MIE data breach ("Nationwide Class").

122. Alternatively, Plaintiffs propose the following subclasses by state or groups of states: "All persons in [NAME OF STATE(S)] whose Personal or Medical Information was compromised by the MIE data breach" ("Statewide Class").

123. The Classes are so numerous that joinder of all members is impracticable. The Classes include 3.9 million individuals whose Personal or Medical Information was compromised by the MIE data breach.

124. There are numerous questions of law and fact common to Plaintiffs and the Members of the Classes, including the following:

1) Whether Defendants failed to adequately safeguard Plaintiffs' and the Classes' Personal and Medical Information;
2) Whether Defendants failed to protect Plaintiffs' and the Classes' Personal and Medical Information, as promised;
3) Whether Defendants' computer systems and data security practices used to protect Plaintiffs' and the Classes' Personal and Medical Information violated HIPAA, federal, state, and local laws, industry practices, or Defendants' duties;
4) Whether Plaintiffs and Class Members are third party beneficiaries to Defendants' Agreements with their Clients;
5) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Personal and Medical Information properly and/or as promised;

6) Whether Defendants violated the consumer protection statutes, data breach notification statutes, and state medical privacy statutes applicable to Plaintiffs and each of the Classes;

7) Whether Defendants failed to notify Plaintiffs and members of the Classes about the MIE data breach as soon as practical and without delay after the MIE data breach was discovered;

8) Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Classes' Personal and Medical Information;

9) Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiffs and the members of the each of the Classes, on the other;

10) Whether Defendants' conduct described herein constitutes a breach of their implied or express contracts with Plaintiffs and the members of each of the Classes;

11) Whether Defendants should retain the money paid by Plaintiffs and members of each of the Classes to Defendant's Clients to protect their Personal and Medical Information;

12) Whether Plaintiffs and the members of the Classes are entitled to damages as a result of Defendants' wrongful conduct; and

13) Whether Plaintiffs and the members of the Classes are entitled to restitution as a result of Defendants' wrongful conduct.

125. Plaintiffs' claims are typical of the claims of the Classes in that the representative Plaintiffs, like all Class members, had their Personal and Medical Information compromised in the MIE data breach.

126. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained counsel who is experienced in class-action and complex litigation. Plaintiffs have no interests that are adverse to, or in conflict with, other members of the Classes.

127. The questions of law and fact common to the Class Members predominate over any questions which may affect only individual members.

128. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy.

129. The prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for MIE. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

COUNT I – THIRD PARTY BENEFICIARY CLAIM FOR BREACH OF CONTRACT BROUGHT BY NATIONWIDE CLASS AGAINST DEFENDANTS

130. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

131. Defendants had a valid, binding, and enforceable express contract with their Clients to provide software and EMR services for the electronic medical records of Plaintiffs and Nationwide Class Members that contained their Personal and Medical Information.

132. Under the express terms of the contract, Indiana law applies to breach of contract claims, and venue is proper in this Court.

133. Under the contract, Defendants promised to "keep confidential and not disclose any . . . Confidential Information . . . to which MIE is permitted access or which is disclosed to MIE . . . ." (Ex. A at 9, ¶ 8.9(b).)

134. Under the contract, Defendants promised to "hold the Confidential Information of the other party in the strictest confidence . . . and not to release or make any portion of it available . . . for copying or use by any third party." (Ex. B at ¶ 10.1.)

135. In Indiana, "all applicable law in force at the time the agreement is made impliedly forms a part of the agreement without any statement to that effect." *Strauss Veal Feeds, Inc. v. Mead & Hunt, Inc.*, 538 N.E.2d 299, 302 (Ind. Ct. App. 1989) (citing *Ethyl Corp. v. Forcum-Lannom Assoc.*, 433 N.E.2d 1214, 1220 (Ind. Ct.

App. 1982)). Therefore, under the contract, Defendants promised to comply with federal and state laws and regulations, including HIPAA, and industry standards.

136. The terms of the contract that concern the protection of Plaintiffs' and Nationwide Class Members' Personal and Medical Information were material terms of the contract.

137. Defendants did not satisfy their promises and obligations to their Clients under the contract because they did not take reasonable and contractually-required measures to hold the Personal and Medical Information of Plaintiffs and Nationwide Class Members in the strictest confidence and to prevent unauthorized third-party access to that information.

138. Defendants did not satisfy their promises and obligations to their Clients under the contract because they did not comply with the applicable federal and state laws and regulations, including HIPAA, and industry standards.

139. Defendants materially breached their contract with their Clients by failing to implement the security measures required by the contracts to hold the Personal and Medical Information of Plaintiffs and Nationwide Class Members in the strictest confidence and to prevent unauthorized third-party access to that information. Instead, Plaintiffs' and Nationwide Class Members' Personal and Medical Information was stored in an inadequately-secured computer system and accessed and exfiltrated by an unauthorized third party.

140. Defendants' Clients fully performed their obligations under the contract and satisfied all conditions, covenants, obligations, and promises of the agreement.

141. Defendants' failure to satisfy their promises and obligations led directly to the MIE data breach, in which Defendants let unauthorized third parties access and exfiltrate Plaintiffs and Nationwide Class Members' Personal and Medical Information.

142. Plaintiffs and Nationwide Class Members are intended third-party beneficiaries of the data security provisions in the contract between Defendants and their Clients and are entitled to directly enforce its terms.

143. The benefits that Plaintiffs and Nationwide Class Members receive under the contract are not incidental to the purpose of the contract. Instead, the purpose of the contract is to define the terms and conditions under which Defendants would provide software and EMR services for the electronic medical records of Plaintiffs and Nationwide Class Members that contained their Personal and Medical Information. The provisions of the contract that pertain to data security are intended to protect the Personal and Medical Information of Plaintiffs and Nationwide Class Members.

144. As a result of Defendants' failure to implement the security measures required by the contract, the Clients did not receive the full benefit of their bargain, and instead Plaintiffs and Nationwide Class Members received health care services that were less valuable because the promised data security was not provided to

secure their Personal and Medical Information, which information formed the very basis of the contract between Defendants and their Clients.

145. Also as a result of Defendants' failure to implement the security measures promised in the contract, Plaintiffs and Nationwide Class Members have suffered actual damages resulting from the theft of their Personal and Medical Information and remain at imminent risk of suffering additional damages in the future. Plaintiffs and Nationwide Class Members also overpaid for health care services, which were in part paid indirectly to Defendants via their Clients because Plaintiffs and Nationwide Class Members did not receive the full benefit of the services that were promised (data security to protect their Personal and Medical Information) and that the Clients intended them to receive.

146. Accordingly, Plaintiffs and Nationwide Class Members have been injured as a result of Defendants' breach of contract and are entitled to damages and/or restitution.

COUNT II – NEGLIGENCE
BROUGHT BY 53 STATEWIDE CLASSES AGAINST DEFENDANTS

147. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

148. Defendants requested and came into possession of the Plaintiffs' and Statewide Class Members' Personal and Medical Information in order to provide electronic medical record services to Defendants' Clients.

149. Defendants knew, or should have known, of the risks inherent in collecting and storing the Personal and Medical Information of Plaintiffs and Statewide Class Members.

150. As described above, Defendants owed duties of care to Plaintiffs and Statewide Class Members whose Personal Information had been entrusted with Defendants.

151. Defendants breached their duties to Plaintiffs and Statewide Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Statewide Class Members' Personal and Medical Information.

152. Defendants acted with wanton disregard for the security of Plaintiffs' and State Class Members' Personal and Medical Information. Defendants knew or should have known that they had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the Personal and Medical Information in computer systems, such as theirs.

153. A "special relationship" exists between Defendants and the Plaintiffs and Statewide Class Members. Defendants entered into a "special relationship" with the Plaintiffs and Statewide Class Members whose Personal and Medical Information was requested, collected, and received by Defendants. Defendants also entered into a "special relationship" by placing their Personal and Medical Information in Defendants' systems—information that Plaintiffs and Statewide

Class Members had been required to provide to MIE's Clients to receive healthcare. Furthermore, Defendants also created a "special relationship" with Plaintiffs and Statewide Class Members by creating and maintaining computer systems that were used for storage of all of Plaintiffs' and Statewide Class Members' Personal and Medical Information.

154. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Statewide Class Members, Plaintiffs and Statewide Class Members would not have been injured.

155. The injury and harm suffered by Plaintiffs and Statewide Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Statewide Class Members to experience the foreseeable harms associated with the exposure of their Personal and Medical Information.

156. As a direct and proximate result of Defendants' negligent conduct Plaintiffs and Statewide Class Members have suffered injury and are entitled to damages.

COUNT III – NEGLIGENCE PER SE
BROUGHT BY 53 STATEWIDE CLASSES AGAINST DEFENDANTS

157. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

158. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Statewide Class Members' Personal and Medical Information.

159. Pursuant to HIPAA's Privacy Rule and Security Rule, Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Statewide Class Members' Personal and Medical Information.

160. Pursuant to state laws in the following states, Defendants had a duty to those respective states' Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information:

1) Arkansas: Ark. Code § 4-110-104
2) California: Cal. Civ. Code § 1798.81.5
3) Florida: Fla. Stat. § 501.171(2)
4) Indiana: Ind. Code § 24-4.9-3-3.5
5) Nevada: Nev. Rev. Stat. § 603A.210
6) Oregon: Or. Rev. Stat. § 646A.622(1)
7) Texas: Tex. Bus. & Com. Code § 521.052(a)

161. Defendants breached their duties to Plaintiffs and Statewide Class Members under the Federal Trade Commission Act, HIPAA, and the state reasonable data security statutes by failing to provide fair, reasonable, or adequate

computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal and Medical Information.

162. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

163. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Statewide Class Members, Plaintiffs and Statewide Class Members would not have been injured.

164. The injury and harm suffered by Plaintiffs and Statewide Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Statewide Class Members to experience the foreseeable harms associated with the exposure of their Personal and Medical Information.

165. As a direct and proximate result of Defendants' negligent conduct Plaintiffs and Statewide Class Members have suffered injury and are entitled to damages.

COUNT IV – BREACH OF CONTRACT
BROUGHT BY 53 STATEWIDE CLASSES AGAINST DEFENDANTS

166. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

167. Plaintiffs and Statewide Class Members had valid, binding, and enforceable express, third party beneficiary, or implied contracts with Defendants as follows:

1) Defendants' promised on their websites to implement security measures to protect Plaintiffs' and Statewide Class Members' Personal Information in accordance with applicable law, regulations, and industry standards.

2) Plaintiffs and Statewide Class Members were required to provide Personal and Medical Information to Defendants' Clients, who received that information under a contractual arrangement. This information was valuable to Defendants because they used it to provide EMR and software services to their Clients. By the Clients' demand and Defendants' acceptance of Plaintiffs' and Statewide Class Members' Personal and Medical Information, Defendants entered into implied contracts with Plaintiffs and Statewide Class Members that required Defendants to take reasonable measures to protect the security and confidentiality of the Personal and Medical Information in accordance with applicable law, regulations, and industry standards.

168. The terms of Plaintiffs' and Statewide Class Members' contracts with Defendants that concern the protection of Plaintiffs' and Statewide Class Members' Personal and Medical Information, set forth above, were material terms of the contracts.

169. Defendants did not satisfy their promises and obligations to Plaintiffs and Class Members under the contracts in that they did not take reasonable measures to keep Plaintiffs' and Statewide Class Members' Personal and Medical Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

170. Defendants materially breached their contracts with Plaintiffs and Statewide Class Members by failing to implement the security measures required by the contracts.

171. Plaintiffs and Statewide Class Members fully performed their obligations under their contracts with Defendants.

172. Defendants' failures to satisfy these promises and obligations led directly to the MIE data breach, in which Defendants let unauthorized parties access and exfiltrate Plaintiffs' and Statewide Class Members' Personal and Medical Information.

173. As a result of Defendants' failure to implement the security measures required by the contracts, Plaintiffs and Statewide Class Members did not receive the full benefit of their bargain, and instead received from Defendants' Clients health care services that were less valuable than what they paid for, which was in part the securing of their Personal and Medical Information entrusted to the Clients and Defendants. Plaintiffs and Statewide Class Members, therefore, were damaged in an amount at least equal to this overpayment.

174. Also as a result of Defendants' failure to implement the security measures required by the contracts, Plaintiffs and Statewide Class Members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

175. Accordingly, Plaintiffs and Statewide Class Members have been injured as a result of Defendants' breach of contract and are entitled to damages and/or restitution.

COUNT V – BREACH OF IMPLIED CONVENANT OF GOOD FAITH AND FAIR DEALING BROUGHT BY 53 STATEWIDE CLASSES AGAINST DEFENDANTS

176. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

177. Plaintiffs and Statewide Class Members entered into valid, binding, and enforceable express, implied, or third-party beneficiary contracts with Defendants, as alleged above.

178. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' and Statewide Class Members'

Personal and Medical Information and to comply with industry standards and federal and state laws and regulations.

179. A "special relationship" exists between Defendants and the Plaintiffs and Statewide Class Members. Defendants entered into a "special relationship" with the Plaintiffs and Statewide Class Members whose Personal and Medical Information was requested, collected, and received by Defendants. Defendants also entered into a "special relationship" by placing their Personal and Medical Information in Defendants' systems—information that Plaintiffs and Statewide Class Members had been required to provide to MIE's Clients to receive health care services. Furthermore, Defendants also created a "special relationship" with Plaintiffs and Statewide Class Members by creating and maintaining computer systems that were used for storage of Plaintiffs' and Statewide Class Members' Personal and Medical Information.

180. Despite these "special relationships" with Plaintiffs and Statewide Class Members, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Statewide Class Members' Personal and Medical Information. For example, instead of implementing reasonable security measures to protect the Personal and Medical Information, Defendants provided wholly inadequate security measures that violated basic information security standards.

181. Plaintiffs and Statewide Class Members fully performed their obligations under their contracts with Defendants.

182. Defendants' failure to act in good faith in implementing the security measures required by the contracts, denied Plaintiffs and Statewide Class Members the full benefit of their bargain, and instead they received from Defendants' Clients health care services that were less valuable than what they paid for, which was in part the securing of their Personal and Medical Information entrusted to the Clients and Defendants. Plaintiffs and Statewide Class Members, therefore, were damaged in an amount at least equal to this overpayment.

183. Defendants' failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Statewide Class Members to suffer actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

184. Accordingly, Plaintiffs and Statewide Class Members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution.

COUNT VI – NEGLIGENT MISREPRESENTATION BROUGHT BY THE 53 STATEWIDE CLASSES

185. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

186. Defendants negligently and recklessly misrepresented material facts to Plaintiffs and Statewide Class Members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs'

and Statewide Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft.

187. Defendants negligently and recklessly misrepresented material facts to Plaintiffs and Statewide Class Members by representing that they did and would comply with the requirements of relevant laws pertaining to privacy and security of Plaintiffs' and Statewide Class Members' Personal and Medical Information.

188. Because of multiple warnings about data breaches and the threat of data breaches to the healthcare industry, Defendants either knew or should have known that their representations were not true.

189. In reliance upon these misrepresentations, Plaintiffs and Statewide Class Members allowed their Personal and Medical Information to be entrusted to Defendants.

190. Had Plaintiffs and Statewide Class Members, as reasonable persons, known of Defendants' inadequate data privacy and security practices, or that Defendants were failing to comply with the requirements of laws pertaining to the privacy and security of Plaintiffs' and Statewide Class Members' Personal Information, they would not have purchased health services from Defendants' Clients, and would not have allowed their Personal and Medical Information to be entrusted to Defendants.

191. As a direct and proximate consequence of Defendants' negligent misrepresentations, Plaintiffs and Class Members have suffered the injuries alleged above.

COUNT VII – UNJUST ENRICMENT
BROUGHT BY 53 STATEWIDE CLASSES

192. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

193. Plaintiffs and Statewide Class Members conferred a monetary benefit on Defendants. Defendants received and retained money belonging to Plaintiffs and Statewide Class Members in the form of fees charged to their health service providers for Defendants' EMR services.

194. Defendants appreciated or had knowledge of the benefits conferred on them by Plaintiffs and Statewide Class Members.

195. The money that Plaintiffs and Statewide Class Members paid indirectly to Defendants were supposed to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

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

197. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Statewide Class

Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

198. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Statewide Class Members all unlawful or inequitable proceeds received by Defendants.

199. A constructive trust should be imposed on all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and Statewide Class Members.

COUNT VIII - VIOLATION OF STATE CONSUMER LAWS BROUGHT BY CERTAIN STATEWIDE CLASSES BELOW

Arkansas
Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §4-88-101 *et seq.*
(Brought by Arkansas Class Against Defendants)

200. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

201. In the course of their businesses, Defendants engaged in deceptive and unconscionable acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of Ark. Code Ann. § 4-88-107, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Arkansas Class by

representing that they would maintain adequate data privacy and security practices and procedures to safeguard Arkansas Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Ark. Code Ann. § 4-88-107(a)–(1), (3), (10);

2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Arkansas Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arkansas Class Members' Personal and Medical Information, in violation of Ark. Code Ann. § 4-88-107(a)–(1), (3), (10);

3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Arkansas Class Members' Personal and Medical Information, in violation of Ark. Code Ann. § 4-88-107(a)–(1), (3), (10); and

4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Arkansas Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15

U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), and the Arkansas Protection of Personal Information Act (Ark. Code Ann. § 4-110-104).

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

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

204. As a direct and proximate result of Defendants' deceptive practices, Arkansas Class Members suffered injury and/or damages.

205. Arkansas Class Members seek relief under Ark. Code Ann. § 4-88-113, including, but not limited to actual damages, and attorneys' fees and costs.

Arizona
Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521, *et seq*.
(Brought by Arizona Class Against Defendants)

206. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

207. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material

facts in connection with the sale and advertisement of "merchandise" (as defined in the Arizona Consumer Fraud Act, A.R.S. §44-1521(5)) in violation of A.R.S. §44-1522(A), including but not limited to the following:

1) Defendants misrepresented material facts to the Arizona Class, in connection with the sale of EMR services and health services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Arizona Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft;
2) Defendants misrepresented material facts to the Arizona Class, in connection with sale of EMR services and health services, by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Arizona Class Members' Personal and Medical Information;
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Arizona Class Members' Personal and Medical Information, with the intent that others rely on the omission, suppression, and concealment;
4) Defendants engaged in unfair acts and practices, in connection with the sale of EMR services and health services by failing to maintain the privacy and security of Arizona Class Members' Personal and Medical Information, in violation of duties imposed by and public policies

reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), and HIPAA (42 U.S.C. § 1302d *et seq*.); and

5) Defendants engaged in unfair acts and practices in connection with the sale of EMR services and health services by failing to disclose the MIE data breach to Arizona Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 44-7501.

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

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

210. As a direct and proximate result of Defendants' unlawful practices, Arizona Class Members suffered injury and/or damages.

211. Arizona Class Members seek relief including, but not limited to, compensatory damages, punitive damages, injunctive relief, and/or attorneys' fees and costs.

California

California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*
(Brought by California Class Against Defendants)

212. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

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

1) Defendants engaged in deceptive acts and practices with regard to the EMR services and health services provided to the California Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard California Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft; representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of California Class Members' Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the

inadequacy of the privacy and security protections for California Class Members' Personal and Medical Information.

2) Defendants engaged in unfair acts and practices with respect to the EMR services and health services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Class Members' Personal and Medical Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Class Members' Personal and Medical Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq*.), California's Confidentiality of Medical Information Act (Cal. Civ. Code §56 *et seq*.), and California's data breach statute, Cal. Civ. Code § 1798.81.5. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

3) Defendants engaged in unfair acts and practices with respect to the sale of EMR services and health services by failing to disclose the MIE data breach to California Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

4) Defendants engaged in unfair acts and practices with respect to the provision of EMR services and health services by failing to take proper action following the MIE data breach to enact adequate privacy and security measures and protect California Class Members' Personal and Medical Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

5) Defendants engaged in unlawful business practices by violating the privacy and security requirements of HIPAA (42 U.S.C. § 1302d *et seq*.).

6) Defendants engaged in unlawful business practices by violating California's Confidentiality of Medical Information Act (Civil Code §56 *et seq*.).

7) Defendants engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

214. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, the Plaintiffs were injured and lost money or property, including but not limited to the overpayments Defendants received from Defendants' Clients to take reasonable and adequate security measures (and they did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above.

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

216. California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq*., including, but not limited to, restitution to Plaintiffs and California Class Members of money or property that the Defendants may have acquired by means of Defendants' deceptive, unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their

unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief.

Florida

Florida Deceptive and Unfair Trade Practices, Fla. Stat. Ann. § 501.201 *et seq.* (Brought by Florida Class Against Defendants)

217. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

218. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of Fla. Stat. Ann. § 501.204, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Florida Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Florida Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Fla. Stat. Ann. § 501.204;
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Florida Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Florida

Class Members' Personal and Medical Information, in violation of Fla. Stat. Ann. § 501.204;

3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Florida Class Members' Personal and Medical Information, in violation of Fla. Stat. Ann. § 501.204;

4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Florida Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), and the Florida Security of Confidential Personal Information statute (Fla. Stat. Ann. § 501.171).

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

220. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Florida Class Members' Personal and Medical Information and that risk of a data breach or theft was highly

likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Florida Class.

221. As a direct and proximate result of Defendants' deceptive practices, Florida Class Members suffered injury and/or damages.

222. Florida Class Members seek relief under Fla. Stat. Ann. § 501.201 *et seq.*, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

Indiana
Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3
(Brought by Indiana Class Against Defendants)

223. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

224. Defendants are "suppliers" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to the purchase and sale of EMR services and health services in Indiana for personal, family, and/or household purposes, in violation of Ind. Code § 24-5-0.5-3, including but not limited to the following:

1) Defendants misrepresented and fraudulently advertised material facts by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Indiana Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft;

2) Defendants misrepresented material facts to the Indiana Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Indiana Class Members' Personal and Medical Information;

3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Indiana Class Members' Personal and Medical Information;

4) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Indiana Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

5) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the MIE data breach to Indiana Class Members in a timely and accurate manner, contrary to the duties imposed by Ind. Code § 24-4.9-3.3.

225. As a direct and proximate result of Defendants' deceptive trade practices, Indiana Class Members suffered injuries, including the loss of their

legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and damages.

226. The above unfair and deceptive practices and acts by Defendants were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under Ind. Code § 24-5-0.5-1 *et seq*.

227. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Indiana Class Members' Personal and Medical Information and that risk of a data breach or theft was highly likely.

228. Indiana Class Members seek relief under Ind. Code § 24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs. Senior Members of the Indiana Class injured by Defendants' unfair and deceptive trade practices also seek treble damages, pursuant to § Ind. Code §24-5-0.5-4(i).

Nevada
Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0915, *et seq.*; Nev. Rev. Stat. § 41.600 *et seq.*
(Brought by Nevada Class Against Defendants)

229. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

230. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and

health services in violation of Nev. Rev. Stat. § 598.0915, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Nevada Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nevada Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915 (5), (7), (9), and (15);
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Nevada Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nevada Class Members' Personal and Medical Information, in violation of Nev. Rev. Stat. § 598.0915 (5), (7), (9), and (15);
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nevada Class Members' Personal and Medical Information, in violation of Nev. Rev. Stat. § 598.0915 (5), (7), (9), and (15);
4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Nevada Class Members' Personal and Medical

Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), the Nevada Confidentiality and Disclosure of Information statute (Nev. Rev. Stat. § 695F.410), and the Nevada data breach statute (Nev. Rev. Stat. Ann. § 603A.210); and

5) Defendants engaged in deceptive trade practices with respect to the sale of health services by failing to disclose the MIE data breach to Nevada Class Members in a timely and accurate manner, in violation of Nev. Rev. Stat. Ann. § 603A.220(1).

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

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

233. As a direct and proximate result of Defendants' deceptive practices, Nevada Class Members suffered injury and/or damages.

234. Nevada Class Members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

New Jersey
New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1, *et seq.*
(Brought by New Jersey Class Against Defendants)

235. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

236. Plaintiffs bring this claim against Defendants on behalf of the New Jersey Class.

237. Defendants sell "merchandise," as meant by N.J. Stat. Ann. § 56:8-1, by offering their services to the public.

238. Defendants engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of their services in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of their services, to the New Jersey Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New Jersey Class Members' Personal and

Medical Information from unauthorized disclosure, release, data breaches, and theft;

2) Defendants misrepresented material facts, pertaining to the sale of their services, to the New Jersey Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Jersey Class Members' Personal and Medical Information;

3) Defendants knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for New Jersey Class Members' Personal and Medical Information with the intent that others rely on the omission, suppression, and concealment;

4) Defendants engaged in unconscionable and deceptive acts and practices with respect to the sale their services by failing to maintain the privacy and security of New Jersey Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d, *et seq*.); and

5) Defendants engaged in unconscionable and deceptive acts and practices with respect to the sale of their services by failing to disclose

the MIE data breach to New Jersey Class Members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a).

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

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

241. As a direct and proximate result of Defendants' unconscionable or deceptive acts and practices, New Jersey Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information.

242. New Jersey Class Members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

New Mexico

New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-1, *et seq.*
(Brought By New Mexico Class Against Defendants)

243. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

244. Plaintiffs bring this claim on behalf of the New Mexico Class.

245. Defendants engaged in unconscionable, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of N.M. Stat. Ann. § 57-12-3, including but not limited to the following:

1) Defendants knowingly misrepresented material facts, pertaining to the sale of EMR services and health services, to the New Mexico Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New Mexico Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft;
2) Defendants knowingly misrepresented material facts, pertaining to the sale of EMR services and health services, to the New Mexico Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Mexico Class Members' Personal and Medical Information;

3) Defendants knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for New Mexico Class Members' Personal and Medical Information;

4) Defendants engaged in unfair, unconscionable, and deceptive acts and practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of New Mexico Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair, unconscionable, and deceptive acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*., the New Mexico Confidentiality of Medical Information statute (N.M. Stat. Ann. § 59A-46-27), and the New Mexico Privacy of Nonpublic Personal Information regulation (N.M. Admin. Code 13.1.3); and

5) Defendants engaged in unfair, unconscionable, and deceptive acts and practices with respect to the sale of EMR services and health services by failing to disclose the MIE data breach to New Mexico Class Members in a timely and accurate manner.

246. The above unfair, unconscionable, and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not

reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

247. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard New Mexico Class Members' Personal and Medical Information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Mexico Class.

248. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, New Mexico Class Members suffered a loss in money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information.

249. New Mexico Class Members seek relief under N.M. Stat. Ann. § 57-12-10, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs, as well as treble damages or $300, whichever is greater.

Ohio

Ohio Deceptive Trade Practices, Ohio Rev. Code Ann. § 4165.01 *et seq.*
(Brought by Ohio Class Against Defendants)

250. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

251. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of Ohio Rev. Code Ann. § 4165.02, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Ohio Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Ohio Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Ohio Rev. Code Ann. § 4165.02 (2), (7), (9);
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Ohio Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Ohio Class Members' Personal and Medical Information, in violation of Ohio Rev. Code Ann. § 4165.02 (2), (7), (9);
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Ohio Class Members' Personal and Medical Information, in violation of Ohio Rev. Code Ann. § 4165.02 (2), (7), (9);

4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Ohio Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), and HIPAA (42 U.S.C. § 1302d, *et seq*.).

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

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

254. As a direct and proximate result of Defendants' deceptive practices, Ohio Class Members suffered injury and/or damages.

255. Ohio Class Members seek relief under Ohio Rev. Code Ann. § 4165.03, including, but not limited to, injunctive relief, other equitable relief, actual damages, and attorneys' fees and costs.

Oregon

Oregon Trade Practices and Antitrust Regulation Act, Ore. Rev. Stat. Ann. § 646.605 *et seq.* (Brought by Oregon Class Against Defendants)

256. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

257. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of Ore. Rev. Stat. Ann. § 646.08, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Oregon Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Oregon Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Ore. Rev. Stat. Ann. § 646.08 (1);
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Oregon Class by representing that they did and would comply with the requirements of relevant

federal and state laws pertaining to the privacy and security of Oregon Class Members' Personal and Medical Information, in violation of Ore. Rev. Stat. Ann. § 646.08 (1);

3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Oregon Class Members' Personal and Medical Information, in violation of Ore. Rev. Stat. Ann. § 646.08 (1);

4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Oregon Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), and HIPAA (42 U.S.C. § 1302d, *et seq*.).

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

259. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Oregon Class Members' Personal and Medical Information and that risk of a data breach or theft was highly

likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Oregon Class.

260. As a direct and proximate result of Defendants' deceptive practices, Oregon Class Members suffered injury and/or damages.

261. Oregon Class Members seek relief Ore. Rev. Stat. Ann. § 646.638including, but not limited to, statutory damages, actual damages, and attorneys' fees and costs.

Pennsylvania

Pennsylvania Unfair Trade Practices, 73 Pa. Stat. Ann. § 201-1, *et seq.*
(Brought by Pennsylvania Class Against Defendants)

262. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

263. Plaintiffs bring this claim against Defendants on behalf of the Pennsylvania Class.

264. The Pennsylvania Class Members directly or indirectly purchased EMR services from Defendants in "trade" and "commerce," as meant by 73 Pa. Stat. Ann. § 201-2, for personal, family, and/or household purposes.

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

1) Defendants misrepresented material facts pertaining to the sale of EMR services and health services to the Pennsylvania Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Pennsylvania Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
2) Defendants misrepresented material facts pertaining to the sale of EMR services and health services to the Pennsylvania Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Pennsylvania Class Members' Personal and Medical Information in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Pennsylvania Class Members' Personal and Medical Information in violation of in violation of 73 Pa. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);
4) Defendants engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Pennsylvania Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state

laws, resulting in the MIE data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d, *et seq*.);

5) Defendants engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of EMR services and health services by failing to disclose the MIE data breach to Pennsylvania Class Members in a timely and accurate manner, in violation of 73 Pa. Stat. § 2303(a); and

6) Defendants engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of EMR services and health services by failing to take proper action following the MIE data breach to enact adequate privacy and security measures and protect Pennsylvania Class Members' Personal and Medical Information from further unauthorized disclosure, release, data breaches, and theft.

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

267. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Pennsylvania Class

Members' Personal and Medical Information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Pennsylvania Class.

268. As a direct and proximate result of Defendants' deceptive acts and practices, the Pennsylvania Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information.

269. Pennsylvania Class Members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual damages or $100 per Class Member, whichever is greater, treble damages, and attorneys' fees and costs.

Texas

Texas Deceptive Trade Practices Act, Tex. Bus. & Comm. Code § 17.41 *et seq.* (Brought by Texas Class Against Defendants)

270. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

271. Plaintiffs bring this claim against Defendants on behalf of the Texas Class.

272. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and

health services in violation of Tex. Bus. & Comm. Code § 17.41 *et seq.*, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Texas Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Texas Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Tex. Bus. & Comm. Code § 17.41 (5), (7), and (9);
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Texas Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Texas Class Members' Personal and Medical Information, in violation of Tex. Bus. & Comm. Code § 17.41 (5), (7), and (9);
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Texas Class Members' Personal and Medical Information, in violation of Tex. Bus. & Comm. Code § 17.41 (5), (7), and (9); and
4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Texas Class Members' Personal and Medical

Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach.

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

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

275. As a direct and proximate result of Defendants' deceptive practices, Texas Class Members suffered injury and/or damages.

276. Texas Class Members seek relief under Tex. Bus. & Comm. Code § 17.50, including, but not limited to, injunctive relief, other equitable relief, damages, and attorneys' fees and costs.

Virginia

Virginia Consumer Protection Act, Va. Code Ann. § 59.1-196 *et seq.*
(Brought by Virginia Class Against Defendants)

277. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

278. In the course of their businesses, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of EMR services and health services in violation of Va. Code Ann. § 59.1-196, including but not limited to the following:

1) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Virginia Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Virginia Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft, in violation of Va. Code Ann. § 59.1-200(A);
2) Defendants misrepresented material facts, pertaining to the sale of EMR services and health services, to the Virginia Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Virginia Class Members' Personal and Medical Information, in violation of Va. Code Ann. § 59.1-200(A);
3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Virginia Class Members' Personal and Medical Information, in violation of Va. Code Ann. § 59.1-200(A);

4) Defendants engaged in deceptive trade practices with respect to the sale of EMR services and health services by failing to maintain the privacy and security of Virginia Class Members' Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), and HIPAA (42 U.S.C. § 1302d, et seq.).

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

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

281. As a direct and proximate result of Defendants' deceptive practices, Virginia Class Members suffered injury and/or damages.

282. Virginia Class Members seek relief Va. Code Ann. § 59.1-204 including, but not limited to, statutory damages, actual damages, and attorneys' fees and costs.

Washington
Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*
(Brought by Washington Class Against Defendants)

283. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

284. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code §19.86.020, including but not limited to the following:

1) Defendants misrepresented and fraudulently advertised material facts pertaining to the EMR services and health services to the Washington Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Washington Class Members' Personal and Medical Information from unauthorized disclosure, release, data breaches, and theft;

2) Defendants misrepresented material facts pertaining to EMR services and health services to the Washington Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Washington Class Members' Personal and Medical Information;

3) Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Washington Class Members' Personal and Medical Information;

4) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Washington Class Members Personal and Medical Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the MIE data breach. These unfair acts and practices violated duties imposed by laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq*.), and the Washington regulations pertaining to Privacy of Consumer Financial and Health Information (Wash. ADC 284-04-300);

5) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the MIE data breach to Washington Class Members in a timely and accurate manner, contrary to the duties imposed by § 19.255.010(1); and

6) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the MIE data breach to enact adequate privacy and security measures and protect Washington Class Members' Personal and Medical Information from further unauthorized disclosure, release, data breaches, and theft.

285. As a direct and proximate result of Defendants' deceptive trade practices, Washington Class Members suffered injury and/or damages.

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

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

288. Washington Class Members seek relief under Wash. Rev. Code § 19.86.090, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

COUNT IX - STATE DATA BREACH STATUTES BROUGHT BY CERTAIN STATEWIDE CLASSES BELOW

California
California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*
(Brought by California Class Against Defendants)

289. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

290. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 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."

291. Defendants are businesses that own, maintain, and license personal information, within the meaning of 1798.81.5, about Plaintiffs and California Class Members.

292. Defendants, to the extent they assert they are not "a provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act," violated Civil Code section 1798.81.5, by failing to implement reasonable measures to protect Class Members' Personal and Medical Information.

293. Businesses that own or license computerized data that includes personal information, including Social Security numbers, are required to notify California residents when their Personal Information has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are

reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

294. Defendants are businesses that own or license computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

295. Plaintiffs' and California Class Members' Personal Information (e.g., Social Security numbers) includes personal information as covered by Cal. Civ. Code § 1798.82.

296. Because Defendants reasonably believed that Plaintiffs' and California Class Members' Personal Information was acquired by unauthorized persons during the MIE data breach, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

297. Thus, by failing to disclose the MIE data breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

298. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5; 1798.82, Plaintiffs and California Class Members suffered damages, as described above.

299. Plaintiffs and California Class Members seek relief under Cal. Civ. Code § 1798.84, including, but not limited to, actual damages and injunctive relief.

Georgia
Ga. Code Ann. § 10-1-912(a) *et seq*.
(Brought by Georgia Class Against Defendants)

300. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

301. Defendants are required to accurately notify Plaintiffs and Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

302. Defendants are businesses that own or license computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

303. Plaintiffs' and Georgia Class Members' Personal Information (e.g., Social Security numbers) includes personal information as covered under Ga. Code Ann. § 10-1-912(a).

304. Because Defendants were aware of a breach of their security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Georgia Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

305. Thus, by failing to disclose the MIE data breach in a timely and accurate manner, Defendants violated Ga. Code Ann. § 10-1-912(a).

306. As a direct and proximate result of Defendants' violations of Ga. Code Ann. § 10-1-912(a), Plaintiffs and Georgia Class Members suffered damages, as described above.

307. Plaintiffs and Class Members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

Kansas
Kan. Stat. Ann. § 50-7a02(a), *et seq.*
(Brought by Kansas Class Against Defendants)

308. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

309. Defendants are required to accurately notify Plaintiffs and Kansas Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused misuse Plaintiffs and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

310. Defendants are businesses that own or license computerized data that includes personal information as defined by Kan. Stat. Ann. § 50-7a02(a).

311. Plaintiffs' and Kansas Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under Kan. Stat. Ann. § 50-7a02(a).

312. Because Defendants were aware of a breach of their security system (that was reasonably likely to have caused misuse of Plaintiffs and Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

313. Thus, by failing to disclose the MIE data breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

314. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiffs and Kansas Class Members suffered damages, as described above.

315. Plaintiffs and Kansas Class Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including, but not limited to, broad equitable relief.

Kentucky
Ky. Rev. Stat. Ann. § 365.732(2) *et seq.*
(Brought by Kentucky Class Against Defendants)

316. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

317. Defendants are required to accurately notify Plaintiffs and Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

318. Defendants are businesses that hold computerized data that includes personal information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

319. Plaintiffs' and Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

320. Because Defendants were aware of a breach of their security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Class Members' Personal Information), Defendants had an obligation to disclose the data

breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

321. Thus, by failing to disclose the MIE data breach in a timely and accurate manner, Defendants violated Ky. Rev. Stat. Ann. § 365.732(2).

322. As a direct and proximate result of Defendants' violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiffs and Kentucky Class Members suffered damages, as described above.

323. Plaintiffs and Kentucky Class Members seek relief under Ky. Rev. Stat. Ann. § 446.070, including, but not limited to actual damages.

Louisiana
La. Rev. Stat. Ann. § 51:3074(A), *et seq.*
(Brought by Louisiana Class Against Defendants)

324. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

325. Defendants are required to accurately notify Plaintiffs and Louisiana Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Louisiana Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

326. Defendants are businesses that own or license computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3074(C).

327. Plaintiffs' and Louisiana Class Members' Personal Information (e.g., Social Security numbers) includes personal information as covered under La. Rev. Stat. Ann. § 51:3074(C).

328. Because Defendants were aware of a breach of their security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

329. As a direct and proximate result of Defendants' violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiffs and Class Members suffered damages, as described above.

330. Plaintiffs and Louisiana Class Members seek relief under La. Rev. Stat. Ann. § 51:3075, including, but not limited to, actual damages.

Michigan
Mich. Comp. Laws Ann. § 445.72(1), *et seq.*
(Brought by Michigan Class Against Defendants)

331. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

332. Defendants are required to accurately notify Plaintiffs and Class Members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

333. Defendants are businesses that own or license computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

334. Plaintiffs' and Class Members' Personal Information (e.g. social security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

335. Because Defendants discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

336. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Class Members suffered damages, as described above.

337. Plaintiffs and Michigan Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine.

New Jersey
New Jersey Stat. Ann. § 56:8-163 *et seq.*
(Brought by New Jersey Class Against Defendants)

338. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

339. Defendants are required to accurately notify Plaintiffs and Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and

Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under New Jersey. Stat. Ann. § 56:8-163.

340. Defendants are businesses that hold computerized data that includes personal information as defined by New Jersey. Stat. Ann. § 56:8-161.

341. Plaintiffs' and Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under New Jersey. Stat. Ann. § 56:8-161.

342. Because Defendants were aware of a breach of their security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by New Jersey. Stat. Ann. § 56:8-163.

343. Thus, by failing to disclose the MIE data breach in a timely and accurate manner, Defendants violated New Jersey. Stat. Ann. § 56:8-163.

344. As a direct and proximate result of Defendants' violations of New Jersey. Stat. Ann. § 56:8-163, Plaintiffs and New Jersey Class Members suffered damages, as described above.

Oregon
Or. Rev. Stat. Ann. § 646A.604(1), *et seq*.
(Brought by Oregon Class Against Defendants)

345. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

346. Pursuant to Or. Rev. Stat. Ann. § 646A.622(1), a business "that maintains records which contain personal information" of a Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

347. Defendants are businesses that maintain records which contain personal information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiffs and Class Members.

348. Defendants violated Or. Rev. Stat. Ann. § 646A.622(1), by failing to implement reasonable measures to protect Class Members' Personal Information.

349. Defendants are required to accurately notify Plaintiffs and Class Members if Defendants become aware of a breach of their data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. Ann. § 646A.604(1).

350. Defendants are businesses that own, maintain, or otherwise possess data that includes consumers personal information as defined by Or. Rev. Stat. Ann. § 646A.604(1).

351. Plaintiffs' and Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under Or. Rev. Stat. Ann. § 646A.604(1).

352. Because Defendants discovered a breach of their security system, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. Ann. § 646A.604(1).

353. As a direct and proximate result of Defendants' violations of Or. Rev. Stat. Ann. §§ 646A.604(1) and 646A.622(1), Plaintiffs and Class Members suffered damages, as described above.

354. Plaintiffs and Oregon Class Members seek relief under Or. Rev. Stat. § 646A.624(3), including, but not limited to, actual damages and injunctive relief.

Virginia
Va. Code Ann. § 18.2-186.6(B), *et seq.*
(Brought by Virginia Class Against Defendants)

355. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

356. Defendants are required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of their data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

357. Defendants are entities that own or license computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

358. Plaintiffs' and Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

359. Because Defendants discovered a breach of their security system (in which unencrypted or unredacted personal information was or is reasonably

believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identity theft or another fraud), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

360. As a direct and proximate result of Defendants' violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Class Members suffered damages, as described above.

361. Plaintiffs and Virginia Class Members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

Washington
Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*
(Brought by Washington Class Against Defendants)

362. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

363. Defendants are required to accurately notify Plaintiffs and Class Members following discovery or notification of the breach of their data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) in the most expedient time possible and without unreasonable delay under Wash. Rev. Code Ann. § 19.255.010(1).

364. Defendants are businesses that own or license computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.010(1).

365. Plaintiffs' and Class Members' Personal Information (e.g., social security numbers) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.010(5).

366. Because Defendants discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1).

367. As a direct and proximate result of Defendants' violations of Wash. Rev. Code Ann. § 19.255.010(1), Plaintiffs and Class Members suffered damages, as described above.

368. Plaintiffs and Washington Class Members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(10)(a), 19.255.010(10)(b) including, but not limited to, actual damages and injunctive relief.

COUNT X - STATE MEDICAL AND HEALTH INFORMATION PRIVACY STATUTES BROUGHT BY CERTAIN STATEWIDE CLASSES BELOW

California

California Confidentiality of Medical Information Act, Cal. Civil Code § 56 *et seq.* (Brought by California Class Against Defendants)

369. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

370. Plaintiffs bring this claim against Defendants on behalf of the California Class.

371. Defendants are "contractors," as defined in Cal. Civil Code §56.05(d), and are "a provider of health care," as defined in Cal. Civil Code §56.06, and are therefore subject to the requirements of the California Confidentiality of Medical Information Act.

372. The California Class includes "patients," as defined by the Confidentiality of Medical Information Act to whom "medical information" in the possession of Defendants pertains, as defined in Cal. Civil Code §§56.05(j) and (k).

373. Defendants disclosed medical information pertaining to members of the proposed California Class to unauthorized persons without first obtaining consent, in violation of Cal. Civil Code §56.10(a).

374. Defendants disclosed medical information pertaining to members of the proposed California Class to unauthorized persons without first obtaining the authorization required by Civil Code §56.11, in violation of that section.

375. Defendants' negligence resulted in the release of individually-identifiable medical information pertaining to members of the California Class to unauthorized persons and the breach of the confidentiality of that information. Defendants' negligent failure to maintain or preserve medical information pertaining to members of the California Class in a manner that preserved the confidentiality of the information contained therein violates Cal. Civil Code §56.06 and §56.101(a).

376. Defendants' electronic health record system or electronic medical record system did not protect and preserve the integrity of electronic medical record information in violation of Civil Code §56.101(b)(1)(A).

377. The California Class were injured and have suffered damages from Defendants' illegal disclosure and negligent release of their medical information in violation of Civil Code §56.10 and §56.101, and therefore seek relief under Civil Code §56.35 and §56.36 including but not limited to actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and/or attorneys' fees, expenses, and costs.

Virginia

Virginia Health Records Privacy Statute, Va. Code § 32.1-127.1:03 (Brought by Virginia Class Against Defendants)

378. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

379. Plaintiffs bring this claim against Defendants on behalf of the Virginia Class.

380. Virginia law recognizes an individual's right of privacy in the content of his or her health records. Va. Code § 32.1-127.1:03.

381. As a result of conducting the business of EMR services in Virginia, Defendants possessed health records pertaining to members of the Virginia Class.

382. Defendants had a duty under Virginia law to not redisclose or otherwise reveal any health records in its possession regarding the Virginia Class. Va. Code § 32.1-127.1:03(3).

383. Defendants redisclosed or otherwise revealed the health records pertaining to the Virginia Class without their consent and for no other reason permitted by Va. Code § 32.1-127.1:03(3), and therefore violated Va. Code § 32.1-127.1:03(3).

384. Virginia Class Members were injured by Defendants' illegal disclosure and negligent release of their health records in violation of Va. Code § 32.1-127.1:03(3).

385. The Virginia Class seeks relief for Defendants' violation of Va. Code § 32.1-127.1:03(3), including but not limited to actual damages, special damages, nominal damages, exemplary damages, injunctive relief, and/or attorneys' fees and costs.

Washington

Washington Uniform Health Care Information Act, Wash. Rev. Code §70.02.045, §70.02.170 (Brought By Washington Class Against Defendants)

386. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

387. Plaintiffs bring this claim against Defendants on behalf of the Washington Class.

388. As a result of conducting the business of EMR services in Washington, Defendants possessed personal information including personal health care information pertaining to members of the Washington Class.

389. Defendants released personal information, including health care information, regarding members of the Washington Class without authorization in violation of Wash. Rev. Code §70.02.045.

390. The Washington Class were injured and have suffered damages from Defendants' illegal disclosure and negligent release of their personal information, including health care information in violation of Wash. Rev. Code §70.02.045.

391. The Washington Class seek relief under Wash. Rev. Code §70.02.170, including but not limited to actual damages, nominal damages, injunctive relief, and/or attorneys' fees and costs.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and the Classes, request that the Court enter judgment against Defendants, as follows:

1. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Classes as requested in this Complaint, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Classes requested in this Complaint.

2. An award of injunctive relief and other equitable relief as is necessary to protect the interests of the Classes.

3. An award to Plaintiffs and the Classes of actual, compensatory, direct, consequential, statutory, punitive, treble, and incidental damages.

4. An award to Plaintiffs and the Classes of equitable relief, restitution, and disgorgement of profits.

5. An award of attorneys' fees, costs, and expenses, as provided by law, or equity, or as otherwise available.

6. An award of pre-judgment and post-judgment interest, as provided by law or equity.

7. Such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: March 22, 2016

Respectfully submitted,

s/ Irwin B. Levin

Irwin B. Levin, No. 8786-49
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Fax: (317) 636-2593
ilevin@cohenandmalad.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I certify that on March 22, 2016, a copy of this document was served on all counsel of record by operation of the Court's electronic filing system.

s/ Irwin B. Levin
Irwin B. Levin
Plaintiffs' Lead Counsel