UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

JAMES YOUNG, on behalf of himself and all others similarly situated, Plaintiff, vs. MEDICAL INFORMATICS ENGINEERING, INC., Defendant.	)	**Class Action Complaint** **Demand for Jury Trial** No. 1:15-cv-00197

CLASS ACTION COMPLAINT

Plaintiff, James Young, by counsel, on behalf of himself and all others similarly situated, alleges:

NATURE OF THE CASE

1. Between approximately May 7, 2015 and May 26, 2015, Defendant Medical Informatics Engineering, Inc. ("MIE") was subject to a data breach (the "MIE data breach"), when hackers stole the personal financial and protected health information of numerous individuals whose information was used in a MIE electronic health record. The personal and financial information obtained by the hackers includes 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, and Social Security number ("PII"). The protected health information obtained by the hackers includes lab results, health insurance policy information, diagnosis, disability code, doctor's name, medical conditions, and child's name and birth statistics ("PHI").

2. MIE's conduct—failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' PII and PHI, and failing to provide timely and adequate notice of the MIE data breach—has caused substantial consumer harm and injuries to consumers across the United States.

3. As a result of the MIE data breach, numerous individuals whose PII and PHI was used in a MIE electronic health record have been exposed to fraud and these individuals have been harmed. The injuries suffered by the proposed Class as a direct result of the MIE data breach include: theft of their PII and PHI; costs associated with the detection and prevention of identity theft and medical identity theft and unauthorized use of their PII and PHI; 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 data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the MIE data breach; the imminent and certainly impending injury flowing from potential fraud and identify theft and medical identity theft posed by their PII and PHI being placed in the hands of hackers; damages to and diminution in value of their PII and PHI

entrusted to MIE for the sole purpose of maintaining electronic health records and with the mutual understanding that MIE would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and continued risk to their PII and PHI, which remains in the possession of MIE and which is subject to further breaches so long as MIE fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

4. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated individuals whose PII and PHI was stolen as a result of the MIE data breach. Plaintiff asserts claims against MIE for violations of Indiana's consumer laws, negligence, breach of implied contract, bailment, and unjust enrichment. On behalf of themselves and all similarly situated consumers, Plaintiff seeks to recover damages, including actual and statutory damages, and equitable relief, restitution, disgorgement, costs, and reasonable attorney fees.

PARTIES

5. Plaintiff James Young resides in Indianapolis, IN. Mr. Young received a letter from MIE informing him that his PII and PHI was compromised as a result of the MIE data breach. Mr. Young was harmed by having his PII and PHI compromised.

6. Plaintiff would not have given, or not allowed MIE to be given, his PII or PHI had MIE told them that it lacked adequate computer systems and data

security practices to safeguard customers' PII and PHI from theft, and had MIE provided them with timely and accurate notice of the MIE data breach.

7. Plaintiff suffered actual injury from having his PII and PHI compromised and stolen in and as a result of the MIE data breach.

8. Defendant MIE is a software developer that provides technical solutions targeted to the healthcare industry. Among other products and services targeted to the healthcare industry, MIE provides an electronic medical record system. MIE is headquartered at 6302 Constitution Drive, Fort Wayne, IN 46804.

JURISDICTION & VENUE

9. 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 Defendant.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because MIE is headquartered here and regularly transacts business here; and some of the Class members reside in this district. The causes of action for the putative Class Members also arose, in part, in this district.

CLASS ACTION ALLEGATIONS

11. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a) and 23(b)(3) are met with respect to the Class defined below.

12. The Plaintiff Class consists of all persons whose PII or PHI was compromised by the MIE data breach.

13. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands, possibly hundreds of thousands, of individuals whose PII and PHI was compromised by the MIE data breach.

14. There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- whether MIE engaged in the wrongful conduct alleged herein;
- whether MIE's conduct was deceptive, unfair, unconscionable and/or unlawful;
- whether MIE owed a duty to Plaintiff and members of the Class to adequately protect their PII and PHI and to provide timely and accurate notice of the MIE data breach to Plaintiff and members of the Class;
- whether MIE breached its duties to protect the PII and PHI of Plaintiff and members of the Class by failing to provide adequate data security and whether MIE breached its duty to provide timely and accurate notice to Plaintiff and members of the Class;
- whether MIE knew or should have known that its computer systems were vulnerable to attack;
- whether MIE's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII and PHI;

- whether MIE unlawfully failed to inform Plaintiff and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard PII and PHI and whether MIE failed to inform Plaintiff and members of the Class of the data breach in a timely and accurate manner;
- whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of MIE's conduct (or failure to act);
- whether Plaintiff and members of the Class are entitled to recover damages;
- whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

15. Plaintiff's claims are typical of the claims of the Class in that the representative Plaintiff, like all Class members, had their PII and PHI compromised in the MIE data breach.

16. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who is experienced in class-action and complex litigation. Plaintiff has no interests that are adverse to, or in conflict with, other members of the Class.

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

18. 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.

19. 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.

FACTS

I. The Healthcare Industry is Put on Notice of Cyber Attacks

20. Companies that provide electronic health record services to the healthcare industry, like MIE, have an obligation to maintain the security of individuals' PII and PHI, which MIE itself recognizes in its Privacy Policy on its website, http://www.mieweb.com/privacy (last visited July 29, 2015):

> Effective Date: February 18, 2010
>
> 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 and in accordance with this Privacy Policy. Please find below details about our practices for handling and securing your personal information. 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. . . .

WHAT INFORMATION DO WE COLLECT?

. . .

2. Personal Information Collection

Medical Informatics Engineering may ask for personal or business information in order to assist us in meeting your various needs, including:

- providing products or services requested;
- servicing your account;
- improving our services; and
- developing and/or informing you of additional products or services that may be of interest

Information sought by Medical Informatics Engineering may depend on the product or service requested. As a result, Medical Informatics Engineering may request personal information including name, street address, ZIP Code, telephone number, fax number, email address, and area of practice or degree (if applicable). Medical Informatics Engineering may collect other personal information through comments, feedback, participation in surveys, or other requests for information.

Further personal information may be required during the application and underwriting process. That information may include, among other things, claim payments, loss history or other underwriting information, credit card numbers, bank account information or social security numbers. In certain circumstances, we may require information primarily used for individual, family or household purposes.

. . .

WHAT INFORMATION DO WE SHARE AND WITH WHOM DO WE SHARE IT?

Medical Informatics Engineering may share personal information with our affiliated companies and third parties for the purpose of fulfilling your requests, or to offer you other products and services that may be of interest to you. Medical Informatics Engineering may or may not receive compensation for sharing such information in this manner.

> Medical Informatics Engineering reserves the right to use this information and to disclose it to others to the extent permitted or required by law, to investigate potential wrongdoing, or to protect the rights, property or safety of Medical Informatics Engineering or others.
> . . .
> 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.
>
> . . .

3. The New York Times reports that "[t]he threat of a hacking is particularly acute in the health care and financial services industry, where companies routinely keep the most sensitive personal information about their customers on large databases." (http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (last visited Feb. 5, 2015).)

4. Indeed, on April 8, 2014, the FBI's Cyber Division issued a public Private Industry Notification titled "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." The notification specifically cautioned that "[c]yber actors will likely increase cyber intrusions against health care systems . . . due to . . . lax cybersecurity standards, and a higher financial payout for medical records in the black market."

5. The FBI cited a report issued in February 2014 by SANS, a leading computer forensics and security firm, warning:

> Health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property. . . . The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

6. By early 2014 computer breaches had become rampant in the healthcare industry, a fact widely disseminated inside and outside the healthcare sector. For example:

- According to a Ponemon Institute report dated March 2013, 63% of the healthcare organizations surveyed reported a data breach during the previous two years. The majority of these breaches resulted in the theft of data. In a March 2014 report, the institute stated that criminal attacks on healthcare companies have increased 100% since 2010.

- An EMC²/RSA White Paper published in 2013 indicated that during the first half of 2013, more than two million healthcare records were compromised, which was 31% of all reported data breaches.

- According to the Identity Theft Resource Center, nearly half of all data breaches so far in 2014 have taken place in the healthcare sector.

- According to a recent analysis of HHS data by the *Washington Post*'s "Wonkblog," the personal data of about 30.1 million people has been affected by 944 recorded "major" health data breaches (defined by HHS as one affecting at least 500 people) since federal reporting requirements under the 2009 economic stimulus package went into effect. This analysis did not include the CHS breach.

- In early 2015, Anthem and was the victim of a data breach that affected nearly 80 million individuals.

- In early 2015, Premera Blue Cross was also the victim of a data breach.

7. Several other studies have shown the healthcare industry to be one of the most affected by and least prepared to deal with hacking attempts. Despite the growing threat, the healthcare industry has been slow to implement improved security measures – slower than other industries handling sensitive information, such as the retail and financial sectors. For instance, the typical healthcare entity allocates only about 2 or 3 percent of its operating budget to its IT department, while retail and financial businesses devote more than 20 percent to IT. According to an annual security assessment conducted by the Healthcare Information and Management Systems Society, almost half of surveyed health systems said they spent 3 percent or less of their IT budgets on security.

II. The MIE Data Breach

8. On June 10, 2015, MIE announced that it was the victim of 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).)

9. On July 23, 2015, MIE provided additional information about the MIE data breach:

> On May 26, 2015, we discovered suspicious activity in one of our servers. We immediately began an investigation to identify and remediate any identified security vulnerability. Our first priority was to safeguard the security of personal and protected health information, and we have been working with a team of third-party experts to investigate the attack and enhance data security and protection. This investigation is ongoing. On May 26, 2015, we also reported this

> incident to law enforcement including the FBI Cyber Squad. Law enforcement is actively investigating this matter, and we are cooperating fully with law enforcement's investigation. The investigation indicates this is a sophisticated cyber attack. Our forensic investigation indicates the unauthorized access to our network began on May 7, 2015. Our monitoring systems helped us detect this unauthorized access, and we were able to shut down the attackers as they attempted to access client data.
>
> We are continuing to take steps to remediate and enhance the security of our systems. Remedial efforts include removing the capabilities used by the intruder to gain unauthorized access to the affected systems, enhancing and strengthening password rules and storage mechanisms, increased active monitoring of the affected systems, and intelligence exchange with law enforcement. We have also instituted a universal password reset.

(http://www.mieweb.com /notice/ (last visited July 29, 2015).)

10. MIE's website then stated that "[w]hile investigations into this incident are ongoing," thus far it has been "determined the security of some personal and protected health information contained on Medical Informatics Engineering's network has been affected. The affected data relating to individuals affiliated with affected Medical Informatics Engineering clients may include 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).)

11. MIE notified the FBI of the breach and the FBI is investigating.

12. MIE detected the breach on May 26, 2015, but did not publicly announce the breach until June 10, 2015.

13. MIE did not start mailing notification to affected individuals until July 17, 2015.

14. MIE's website states that "[t]he following healthcare providers were affected by the Medical Informatics Engineering cyber attack":

- 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.)

15. MIE's website also states that "[i]ndividuals 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 may be affected. The database relating to these healthcare providers was accessed on May 26, 2015. Individuals may also visit the providers' websites, which may be accessed at www.fwradiology.com, for information on this incident."

16. MIE's website also states that "[a]ffected individuals 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

17. MIE's website also provides "[f]raud prevention tips" that show just how damaging the MIE data beach is to class members:

> We suggest affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements for suspicious activity. We also encourage affected individuals to notify their credit card companies, health care providers, and heath care insurers of this data security incident. Affected individuals may also review explanation of benefits statement(s) that they receive from their healthcare provider or health plan. If an affected individual sees 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). If an affected individual does not receive regular explanation of benefits statement(s), we suggest

> he/she contact his/her healthcare provider or health plan and ask that they send a copy after each visit the affected individual makes with his/her health care provider.
>
> We also suggest that affected individuals carefully review their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.
>
> At no charge, individuals can also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify the his/her identity prior to granting credit in his/her name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity.

(http://www.mieweb.com/notice/ (last visited July 29, 2015).)

COUNT I – NEGLIGENCE

18. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

19. MIE owed a duty to Plaintiff and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing MIE's security systems to ensure that Plaintiff's and Class members' PII and PHI in MIE's possession was adequately secured and protected. MIE further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

20. MIE owed a duty, as articulated in in its own Privacy Policy, to protect its customers' PII and PHI.

21. MIE owed a duty to timely disclose the material fact that MIE's computer systems and data security practices were inadequate to safeguard individuals' PII and PHI.

22. MIE breached these duties by the conduct alleged in the Complaint by, including without limitation, (a) failing to protect its customers' PII and PHI; (b) failing to maintain adequate computer systems and data security practices to safeguard customers' PII and PHI; (c) failing to disclose the material fact that MIE's computer systems and data security practices were inadequate to safeguard customers' PII and PHI; and (d) failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the MIE data breach.

23. The conduct alleged in the Complaint caused Plaintiff and Class members to be exposed to fraud and be harmed. The injuries suffered by the Plaintiff and the proposed Class as a direct result of the MIE data breach include: theft of their PII and PHI; costs associated with the detection and prevention of identity theft and medical identity theft and unauthorized use of their financial accounts and medical identity; 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 data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits

on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the MIE data breach; the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and PHI being placed in the hands of hackers; damages to and diminution in value of their PII and PHI entrusted to MIE with the mutual understanding that MIE would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and continued risk to their PII and PHI, which remains in the possession of MIE and which is subject to further breaches so long as MIE fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

COUNT II – BREACH OF IMPLIED CONTRACT

24. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

25. When Plaintiff and members of the Class provided their PII and PHI to MIE, Plaintiff and members of the Class entered into implied contracts with MIE pursuant to which MIE agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

26. Plaintiff and Class members would not have provided and entrusted their PII and PHI to MIE in the absence of the implied contract between them and MiE.

27. Plaintiff and members of the Class fully performed their obligations

under the implied contracts with MIE.

28. MIE breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the PII and PHI of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their PII and PHI was compromised in and as a result of MIE data breach.

29. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of MIE's breaches of the implied contracts between MIE and Plaintiff and members of the Class.

COUNT III – BREACH OF CONTRACT

30. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

31. MIE has a contractual obligation to maintain the security of its customers' PII and PHI, which MIE itself recognizes in its Privacy Policy.

32. MIE breached that contractual obligation by failing to safeguard and protect the PII and PHI of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their PII and PHI was compromised in and as a result of MIE data breach.

33. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of MIE's breaches of the contracts between MIE and Plaintiff and members of the Class.

COUNT IV – BAILMENT

34. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

35. In having their PII and PHI delivered to MIE for the purposes of electronic health records, Plaintiff and Class members intended and understood that MIE would adequately safeguard their personal and financial information.

36. MIE accepted possession of Plaintiff's and Class members' PII and PHI for the purpose of providing electronic health record services.

37. By accepting possession of Plaintiff's and Class members' PII and PHI, MIE understood that Plaintiff and Class members expected MIE to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

38. During the bailment (or deposit), MIE owed a duty to Plaintiff and Class members to exercise reasonable care, diligence, and prudence in protecting their PII and PHI.

39. MIE breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII and PHI, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII and PHI.

40. MIE further breached its duty to safeguard Plaintiff's and Class members' PII and PHI by failing to timely and accurately notify them that their information had been compromised as a result of the MIE data breach.

COUNT V –

VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT

41. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

42. MIE's conduct as alleged in this Complaint violated Ind. Code § 24-5-0.5-3(b)(1), (2), including without limitation that (a) MIE represented that it protected its customers' PII and PHI, but MIE failed to protect that sensitive information; (b) MIE's failure to maintain adequate computer systems and data security practices to safeguard customers' PII and PHI; (c) MIE's failure to disclose the material fact that MIE's computer systems and data security practices were inadequate to safeguard customers' PII and PHI from theft; and (d) MIE's failure to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the MIE data breach.

43. Plaintiff and Class members relied on MIE's misrepresentations.

44. MIE's deceptive acts 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*.

45. Plaintiff and Class members are entitled to $1,000 or treble damages, reasonable attorneys' fees, costs of suit, an ordering enjoining MIE's unlawful practices, and any other relief which the Court deems proper.

COUNT VI – UNJUST ENRICHMENT

46. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

47. Plaintiff and Class members conferred a benefit on MIE by way of customers' paying MIE to maintain Plaintiff and Class members' PII and PHI.

48. The monies paid to MIE were supposed to be used by MIE, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

49. MIE failed to provide reasonable security, safeguards, and protections to the PII and PHI of Plaintiff and Class members, and as a result MIE was overpaid.

50. Under principles of equity and good conscience, MIE should not be permitted to retain the money because MIE failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' PII and PHI that they paid for but did not receive.

51. MIE wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

52. MIE's enrichment at the expense of Plaintiff and Class Members is and was unjust.

53. As a result of MIE's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by MIE, plus attorneys' fees, costs, and interest thereon.

RELIEF REQUESTED

Plaintiff, on behalf of himself and all others similarly situated, request that the Court enter judgment against MIE, as follows:

1. An award to Plaintiff and the Class of compensatory, direct, consequential, statutory, and incidental damages;

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

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

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

DEMAND FOR JURY TRIAL

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

Dated: July 29, 2015

Respectfully submitted,

/s/ Irwin B. Levin

Irwin B. Levin, No. 8786-49
Richard E. Shevitz, No. 12007-49
Vess A. Miller, No. 26495-53
Lynn A. Toops, No. 26386-49A
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Fax: (317) 636-2593
ilevin@cohenandmalad.com
rshevitz@cohenandmalad.com
vmiller@cohenandmalad.com
ltoops@cohenandmalad.com

Counsel for Plaintiff and the Proposed Plaintiff Class