UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

TIFFANY PFLUM, individually and on behalf of all others similarly situated, Plaintiff, v. MUNSON HEALTHCARE, Defendant.	:	CIVIL ACTION Case No.: Hon.

CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL

Plaintiff Tiffany Pflum ("Plaintiff" or "Ms. Pflum"), on behalf of herself individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Munson Healthcare ("Defendant"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. The Defendant in this action is a healthcare provider and, as such, it is entrusted with some of the most sensitive and personal information imaginable. Applicable law and industry standards require Defendant to implement security measures sufficient to protect such information from disclosure to hackers or other unauthorized parties. Defendant failed to meet the necessary requirements, and Plaintiff brings this class action to redress the harm caused by Defendant's failures.

2. Defendant operates nine hospitals in northern Michigan, providing healthcare to approximately half-a-million people. In the course of its business, Defendant collects patient data

and maintains databases of sensitive and personal information obtained from its patients, including Plaintiff and the Class (defined below).

3. Defendant failed to implement adequate technical safeguards and train its employees to protect the confidential information of its patients. Because of this, Defendant allowed the sensitive personal information of at least 75,000 of Defendant's patients to be accessed by unauthorized third parties (the "Breach"). This personal information included Defendant's patients' financial information (*e.g.*, credit card numbers and bank account information), medical information (including treatment and diagnostic information, as well as insurance information), personal information (*e.g.*, Social Security numbers and addresses), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Personal Identifiable Information" or "PII").

4. The Breach occurred when, starting in July of 2019, a stunning twenty-nine of Defendant's employees fell prey to a phishing scheme and allowed unauthorized third parties access to their email inboxes. These email inboxes, in turn, contained extensive PII of Defendant's clients including, among other things, financial information, treatment and diagnostic information, and driver's license and Social Security numbers. When asked why so much PII could potentially be available in an email inbox, Defendant told a reporter for the Cadillac News that email was a useful tool for a healthcare system that spanned several counties.[1] Despite this company-wide reliance on email, however, Defendant failed to implement

[1] Karen Hopper Usher, *Data breach at Munson leaks patient records*, CADILLAC NEWS, (Feb. 27, 2020), *available at* https://www.cadillacnews.com/news/data-breach-at-munson-leaks-patient-records/article_661d3882-0b76-51d2-a309-26b7f11eea4e.html (last visited April 27, 2020).

adequate technical safeguards for its email system and to adequately train its staff to avoid basic phishing schemes.

5. According to Defendant, the hospital was "responding all along" to the phishing attack and brought in a third-party security team in the first week of August.[2] Despite this, email accounts were exposed between July 31 and October 22, 2019, and it wasn't until January 16, 2020 that investigators "concluded their investigation" and found exposed email accounts contained PII. One month later, Plaintiff and the Class members were notified for the first time.

6. On February 26, 2020, Defendant announced the Breach, which it stated it "discovered on January 16, 2020" (the "2020 Notice"). On or around the date of the 2020 Notice, Defendant mailed notification letters to patients impacted or potentially impacted by the Breach.

7. Plaintiff Tiffany Pflum received one of these letters in early March, though she had learned of the breach from local news services at the end of February.

8. Defendant's security failures enabled the criminals behind the Breach to steal PII from Defendant's computer systems and put Plaintiff and the Class members at serious and ongoing risk of identity theft. Defendant's acts and omissions have caused ongoing loss to Plaintiff and Class members from, *inter alia*, the significant time spent attempting to address, mitigate, and monitor the present and future consequences of the Breach, including, as appropriate, review of records for fraudulent charges and healthcare services billed for but not received, cancellation and reissuance of payment cards, purchase of credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, implementation and maintenance of credit freezes, and the stress of managing issues resulting from the Breach.

[2] *Id.*

9. The Breach was caused and enabled by Defendant's violation of its obligations under the law and failure to abide by industry standards and its own policies in regard to implementing adequate security measures. Had Defendant implemented adequate security measures, the Breach could have been prevented or mitigated. Defendant was aware healthcare providers were targeted by cybercriminals and, in fact only a year earlier, had been targeted by unauthorized third-parties who were causing Munson Healthcare numbers and identifying information to appear on caller IDs as part of a phone-phishing scam. [3]

10. As a result of Defendant's actions, Plaintiff has been forced to take remedial steps to protect herself from future loss, including by dedicating significant time that she otherwise would not have in making frequent checks of her accounts and credit to ensure that they are not compromised. Indeed, all of the Class members are currently at a very high risk of fraud or identity theft, and it is reasonable and necessary for them to take prophylactic protective measures, like the purchase of a credit monitoring service, to prevent and mitigate future loss.

11. Defendant's wrongful actions and/or inaction constitute common law negligence, and Plaintiff brings claims of negligence per se, negligent misrepresentation, violation of the Michigan Data Breach Prompt Notification Law, unjust enrichment, breach of contract, and breach of implied contract.

12. Plaintiff, on behalf of herself and on behalf of the Class, seeks damages, injunctive relief, and attorneys' fees and costs.

[3] Munson Healthcare, Phone Scam Spoofs Munson Healthcare Numbers (Nov. 11, 2018) *available at* https://www.munsonhealthcare.org/about-the-system/news-media-relations/news/news-details?news=748 (last visited April 27, 2020).

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) in that: (1) this is a class action involving more than 100 class members; (2) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; and (3) at least one member of the proposed class is a citizen of a state different from Defendant.

14. This Court has personal jurisdiction over Defendant because Defendant does business in and throughout the State of Michigan, and the wrongful acts alleged in this Complaint were committed in Michigan.

15. Venue is proper in this District pursuant to (1) 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class members' claims also occurred in this District.

PARTIES

16. Plaintiff is an individual who works at an after school program in Traverse City, Michigan and who resides in Traverse City, Michigan.

17. Defendant Munson Healthcare is a not-for-profit corporation organized and existing under the laws of the State of Michigan with a principal place of business located at 1105 Sixth Street, Traverse City, Michigan, 49684.

FACTUAL ALLEGATIONS

A. Background

18. Personal Identifiable Information is a valuable commodity. It is sought by legitimate businesses to help better understand the market and target advertising, but it is also coveted by criminals who use it to commit fraud and theft.

19. The Federal Trade Commission ("FTC") has recognized that consumer data is a new and valuable form of currency. Pamela Jones Harbour, former Commissioner of the FTC, observed that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[4]

Indeed, consumers' personal data supports a $26 billion per year online advertising industry in the United States.[5]

20. Criminals also value PII as a means to commit theft (using, for example, stolen bank account information) or to effectuate identity fraud (with the help of, *e.g.*, a Social Security number, name, and address).

21. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[6] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[4] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited April 27, 2020).

[5] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, WALL STREET JOURNAL (Feb. 28, 2011), *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited April 27, 2020).

[6] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited April 27, 2020).

22. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[7]

23. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/financial fraud.

24. There may be a time lag between when PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

25. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver 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.

---

7 *Id.* at 2, 9.

8 *Id.* at 29.

Identity thieves 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.[9]

26. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "deep web" black market for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various websites making the information publicly available.

27. 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.[10]

28. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value—whereas a stolen Social Security number, on the other hand, only sells for $1."[11]

29. A recent survey conducted by Black Book Research ("Black Book Study") found that, of the 733 healthcare organizations surveyed, 93 percent had experienced a data breach in the last three years. "Not only has the number of attacks increased; more than $300 million of

---

[9] *See* Federal Trade Commission, Warning Signs of Identity Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited April 27, 2020).

[10] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited April 27, 2020).

[11] *See Study; Few Aware of Medical Identity Theft Risk*, CLAIMS JOURNAL (June 14, 2012), *available at* http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited April 27, 2020).

records have been stolen since 2015, affecting about one in every ten healthcare consumers." The report further found that providers were the most targeted in the healthcare sector: four out of five breaches affected providers.[12].

30. The Black Book Study merely confirms something that has been widely known for years: cybercriminals target healthcare providers. A 2015 data breach report issued by the credit reporting company Experian repeatedly warns that healthcare providers are susceptible to cybercrime:

> We expect healthcare breaches will increase — both due to potential economic gain and digitization of records. Increased movement to electronic medical records (EMRs), and the introduction of wearable technologies introduced millions of individuals into the healthcare system, and, in return increased, the potential for data breaches. Healthcare organizations face the challenge of securing a significant amount of sensitive information stored on their network, which combined with the value of a medical identity string makes them an attractive target for cybercriminals.[13]

31. Similarly, The New York Times has reported that "[t]he threat of a hacking is particularly acute in the health care and financial services industries, where companies routinely keep the most sensitive personal information about their customers on large databases."[14]

32. The type of data stored by healthcare providers, which is the type of data stolen in the Breach, is far more valuable to identity thieves than credit card information and other PII

---

[12] Jessica Davis, *Data Breaches Will Cost Healthcare $4Bin 2019, Threats Outpace Tech*, CYBERSECURITY NEWS (Nov. 5, 2019), available at: https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last visited April 27, 2020).

[13] Experian, *2015 Second Annual Data Breach Industry Forecast* (2015), *available at* https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last visited April 27, 2020).

[14] *See* Reed Abelson & Matthew Goldstein, *Millions of Quest Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 10, 2015), *available at* https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (last visited April 27, 2020).

stolen from retailers and other businesses that store customer information. While a credit card can be easily cancelled or replaced, these other forms of sensitive PII cannot. Moreover, "Fraudsters can use this data to create fake IDs to buy medical equipment or drugs, or combine a patient number with a false provider number and file fictional claims with insurers."[15] For this reason, "Medical information can be worth ten times more than credit card numbers on the deep web."[16]

33. Because healthcare providers amass large troves of PII, including highly desirable medical information, they must be vigilant in ensuring that patient data are protected from hackers and other cybercriminals and that outside vendors and businesses are not permitted to access patients' information.

34. As a corollary to the uses for PII described above, consumers value keeping their PII private. Researchers have shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

35. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns

---

[15] Aatif Sulleyman, *NHS Cyber Attack: Why Stolen Medical Information is so Much More Valuable than Financial Data*, INDEPENDENT (Friday May 12, 2017), *available at* https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html (last visited April 27, 2020).

[16] *Id.*

[17] Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited April 27, 2020); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[18]

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

B. Defendant Failed to Protect the PII of Plaintiff and the Class from Cybercriminals

37. Defendant offers healthcare services to patients throughout its nine hospitals and related organizations.

38. These services encompass the storage and maintenance of electronic data containing PII, including that of Plaintiff and the Class.

39. On February 26, 2020, Defendant announced that "[a]fter an extensive forensic investigation and comprehensive manual document review," it become aware on January 16, 2020 that certain employee email accounts were accessed by unauthorized third-parties between July 31 and October 22, 2019.[19] The 2020 Notice explained that "[a]ffected email accounts contained the personal and protected health information of certain patients, including their names, dates of birth, insurance information, and treatment and diagnostic information. A limited number of individuals' financial account numbers, driver's license numbers and Social Security numbers were also contained in the impacted email accounts."[20]

40. Despite the 2020 notice, Defendant has also maintained that it was "responding all along" to the phishing attack and brought in a third-party security team in the first week of

[18] *Id.*

[19] Munson Healthcare, *Munson Healthcare Notifies Patients of Data Security Incident* (Feb.26, 2020), *available at* https://www.munsonhealthcare.org/about-the-system/news-media-relations/news/news-details?&news=1030 (last visited April 27, 2020).

[20] Karen Hopper Usher, *supra, note 1.*

August.[21] Despite this knowledge and the workings of both the hospital and outside security teams, email accounts were exposed between July 31 and October 22, 2019, and it wasn't until January 16, 2020 that investigators "concluded their investigation" and found exposed email accounts contained PII. One month later, Plaintiff and the Class members were notified for the first time.

41. According to the breach registry maintained on the Department of Health and Human Services website, the Breach impacted 75,202 individuals.[22]

42. As discussed in more detail below, Defendant represented to Plaintiff and the Class members that their PII was safe with Defendant. Defendant's failure to institute appropriate protective measures regarding the PII stolen in the Breach is especially egregious because it is well known that PII is a valuable commodity that is coveted by cyber criminals, who regularly attack organizations that posses large collections of such data, and that medical-and-health-related data is among the most valuable kind of PII. Defendant should have known it was likely to be targeted by cyber criminals—and had indeed already been targeted as part of a phone phishing scam—and should have had appropriate safeguards in place to protect the PII in its possession.

C. Defendant Represented that It Was Adequately Safeguarding Its Patients' PII

43. Defendant represented that all patient PII it collected, whether in connection with a provider visit or through Defendant's website, would be adequately protected from unlawful disclosure. In various polices discussed below, Defendant described its obligations and

[21] *Id.*

[22] U.S. Department of Health and Human Services, Office of Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited April 27, 2020).

commitments to patient privacy and detailed some of the security measures purportedly protecting PII from disclosure.

44. HIPAA requires Defendant to provide each patient a notice of privacy practices.[23] Defendant's own Notice of Privacy Practices Policy references this obligation, providing that:

> We are required by law to maintain the privacy of individually identifiable patient health information (this information is "protected health information" and is referred to herein as "PHI.") We are also required to provide patients with copy of our Notice of Privacy Practices (NOPP) upon request, and to offer a copy of the Notice at least one time during registration. We will only use or disclose your PHI as permitted or required by applicable state law.[24]

45. The Notice of Privacy Practices also represents that "[t]he State law of Michigan is more stringent than HIPAA in several areas. State law is more stringent when the individual is entitled to greater access to records than under HIPAA and when under state law the records are more protected from disclosure than under HIPAA. Certain federal laws also are more stringent than HIPAA. Munson will continue to abide by these more stringent state and federal laws."[25]

46. Defendant further maintains "Munson understands your health information is highly personal, and we are committed to safeguarding your privacy."[26]

47. Defendant made similar representations regarding the safety of information submitted by patients via Defendant's website. Defendant's Website Privacy Policy assures the reader that, "we take the issue of privacy very seriously and value the trust you place in us each

---

[23] 45 C.F.R § 164.520.

[24] Munson Healthcare, *Notice of Privacy Practices Policy* (revised November 2018), *available at* https://www.munsonhealthcare.org/patients-visitors/notice-of-privacy-practices (last visited April 27, 2020).

[25] *See id.*

[26] *See id.*

time you use our services and access this website."[27] The policy further states: "We will notify you at the time of data collection or transfer if your data will be shared with a third party and you will always have the option of not permitting the transfer. If you do not wish to allow your data to be shared, you can choose not to provide that information or use a particular service."

48. Also relevant to the matter at hand is Defendant's Data Protection Policy. In relevant part, the Data Protection Policy notes "[s]pecial rules apply to the transmission of confidential information via email." While those special rules are not articulated in publicly available documents, the formulation of special rules reveals Defendant's understanding that there are special vulnerabilities when sending confidential information via email.[28] Indeed, experts have long warned about the dangers of sending important private information, like social security numbers, via email.[29]

49. When asked why so much personal information could potentially be available in an email inbox, Defendant told a reporter for the Cadillac News that email was a useful tool for a healthcare system that spanned several counties.[30] Despite this reliance, Defendant failed meet its obligations to safeguard the PII it collected and stored. For example, Defendant failed to employ

---

[27] Munson Healthcare, Website Privacy Statement, *available at* https://www.munsonhealthcare.org/about-the-system/website-privacy-policy# (last visited April 27, 2020).

[28] Munson Healthcare, Data Policy, *available at* https://www.munsonhealthcare.org/media/file/Munson%20Information%20Security%20Policy.pdf (last visited April 27, 2020).

[29] *See e.g.* Rachel Bowie, *5 things you should never send over email or text if you don't want your identity to be stolen*, BUSINESS INSIDER (Mar. 10, 2017), *available at* https://www.businessinsider.com/how-not-to-get-your-identity-stolen-2017-3 (last visited April 27, 2020).

[30] Karen Hopper Usher, *Data breach at Munson leaks patient records*, CADILLAC NEWS, (Feb. 27, 2020), *available at* https://www.cadillacnews.com/news/data-breach-at-munson-leaks-patient-records/article_661d3882-0b76-51d2-a309-26b7f11eea4e.html (last visited April 27, 2020).

complex data encryption (which prevents data that has been accessed or stolen from being readable or otherwise useful) for emails containing PII and failed to adequately train its employees in cybersecurity matters (such as how to spot a phishing attack).[31] If Defendant had encrypted emails containing PII, even if cyber attackers accessed the employee emails, the cyber attackers would not have been able to read them. Similarly, if Defendant's employees had two-factor authentication to access their email, it is unlikely that cyber attackers could have carried out the Breach. Defendant has stated that it will implement additional "technical safeguards" to avoid future occurrences but has not specified what those are.[32] While Defendant framed the implementation of these additional safeguards as a response to the evolution of cybercrimes, phishing scams are not new, and basic prophylactic measures like encryption and two-factor authentication are well established.

50. Defendant also failed to implement adequate monitoring and auditing systems as the email accounts were open to unauthorized third parties for almost three months—this despite the fact that Defendant apparently knew about the phishing scheme as early as August of 2019.

51. At all relevant times, Defendant was legally obligated to protect the PII of Plaintiff and the Class and, in the event of a breach of that data, to timely notify Plaintiff and the

[31] Defendant was on notice that the federal government was concerned about healthcare company data encryption. The United States Department of Health and Human Services' Office for Civil Rights urges health care providers and insurers to encrypt 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' 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." Jim Finkle, FBI warns healthcare firms that they are targeted by hackers, REUTERS (Aug. 2014, 4:32 PM), *available at* http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbiidUSKBN0GK24U20140820.

[32] Munson Healthcare, *Munson Healthcare Notifies Patients of Data Security Incident* (Feb.26, 2020), *available at* https://www.munsonhealthcare.org/about-the-system/news-media-relations/news/news-details?&news=1030 (last visited April 27, 2020).

Class of such a breach. Defendant's failure to institute appropriate protective measures regarding the PII stolen in the Breach is especially egregious because it is well known that PII is a valuable commodity that is coveted by cybercriminals, who regularly attack organizations that possess large collections of such data, and that medical- and health-related data is among the most valuable kinds of PII. Defendant should have known it was likely to be targeted by cybercriminals—and indeed had already been targeted as part of a phone phishing scam—and should have had appropriate safeguards in place to protect the PII in its possession.

D. Defendant Was Required by Law to Protect the PII of Plaintiff and the Class

52. Defendant also violated duties owed to Plaintiff and the Class members under federal law, including HIPAA and the Federal Trade Commission Act.

53. HIPAA and implementing regulations require Defendant to establish procedures to keep secure certain PII it possesses, including, without limitation, names and Social Security Numbers. HIPAA requires Defendant to implement reasonable safeguards for such information, which Defendant failed to do.[33]

54. Defendant failed to honor its obligations under the law and the duties created by its own policies and promises and representations to Plaintiff and the Class by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiff's and the Class members' PII;

[33] *See* 45 C.F.R. § 164.530(c)(1); 45 C.F.R. § 164.306(a) ("Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or 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 . . . .").

c. Ensuring the confidentiality and integrity of electronic protected health information it created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing 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, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the electronically protected health information security standard rules by its workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of its workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

55. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential information.

56. Defendant's data security obligations and promises were particularly important given the substantial increase in data breaches—particularly those impacting the healthcare industry—during the past five years, which were widely known to the public and to anyone in Defendant's industries. Given that Defendant operates in an industry plagued by data breaches and possessed a large trove of valuable data, it was or should have been aware that it was a likely target for cybercriminals.

57. Indeed, in 2018, Defendant alerted customers that unauthorized third-parties were causing Munson Healthcare numbers and identifying information to appear on caller IDs as part of a phone-phishing scam. [34]

58. Because of the wealth of information stored on their systems, healthcare providers such as Defendant are or should be aware that they are prime targets for cybercriminals looking for valuable PII.

[34] Munson Healthcare, Phone Scam Spoofs Munson Healthcare Numbers (Nov. 11, 2018) *available at* https://www.munsonhealthcare.org/about-the-system/news-media-relations/news/news-details?news=748 (last visited April 27, 2020).

59. Defendant was, or should have been, aware of these facts, but failed to institute appropriate safeguards to keep the PII within its possession and control safe from cybercriminals.

E. Plaintiff and the Class Members have been Injured by the Disclosure of their PII

60. Some portion of the monies paid by Plaintiff and the Class to Defendant for medical services was compensation for Defendant's compliance with industry-standard measures with respect to the collection and safeguarding of their PII—or, put another way, the cost of protecting the PII of Plaintiff and the Class was "baked in" to the price Defendant charged for its services. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class overpaid Defendant and thereby incurred actual monetary damages. Plaintiff would have obtained medical services from other suitable providers had Defendant disclosed that it failed to maintain adequate computer systems and data security practices to safeguard Plaintiff's PII from theft. Plaintiff obtained medical services from Defendant in the past three years.

61. Plaintiff and the Class have suffered additional injury in fact and actual damages including from the substantial lost time in monitoring their accounts and credit history (and in otherwise addressing the Breach) that they have spent as a result of the Breach and that they would not have in its absence. For example, since receiving notification of the Breach, Plaintiff now constantly (at least once a day) monitors her credit card transactions and credit history on Credit Karma, which she did not have reason to do before the Breach. Moreover, she has noticed a substantial uptick in spam calls and spam emails since the Breach, which entails further outlays of time and interferes with her use and enjoyment of both communication systems.

62. Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft, the increased risk of identity theft caused by Defendant's wrongful conduct, and the cost of acquiring credit monitoring services.

CLASS ALLEGATIONS

63. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class defined as follows**:**

> All persons whose PII was maintained by Defendant and that was compromised as a result of the Breach publicly disclosed in or about January 2020 (the "Nationwide Class").

64. In addition to and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following Subclass:

> All residents of Michigan whose PII was maintained by Defendant and that was compromised as a result of the Breach publicly disclosed in or about January 2020 (the "Michigan Subclass," collectively with the Nationwide Class, the "Class").

65. The Class is so numerous that joinder of all members is impracticable. The Class has tens of thousands of members. Moreover, the disposition of the claims of the Class in a single action will provide substantial benefits to all parties and the Court.

66. There are numerous questions of law and fact common to Plaintiff and the Class members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's data security systems prior to the Breach complied with all applicable legal requirements;

b. Whether Defendant's data security systems prior to the Breach met industry standards;

c. Whether Plaintiff's and other Class members' PII was compromised in the Breach; and

d. Whether Plaintiff and other Class members are entitled to damages as a result of Defendant's conduct.

67. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of other Class members.

68. Plaintiff's claims are typical of the claims of the Class members. Plaintiff suffered the same injury as the Class members—*i.e.*, upon information and belief, Plaintiff's PII was compromised in the Breach.

69. Defendant has engaged in a common course of conduct toward Plaintiff and other Class members. The common issues arising from this conduct that affect Plaintiff and the Class members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

70. A class action is the superior method for the fair and efficient adjudication of this controversy. The Class members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and publicly available records will easily identify the Class members. The same common documents and testimony will be used to prove Plaintiff's claims as those of the Class.

71. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to the Class members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class members.

COUNT I
NEGLIGENCE

72. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

73. Defendant required Plaintiff and the Class members to submit non-public PII, including names, addresses, credit card information, and Social Security numbers, to obtain medical services, and in the course of Defendant's business it generated and stored highly sensitive medical and health-related information pertaining to Plaintiff and the Class members.

74. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and the Class.

75. Defendant had a duty of care to use reasonable means to secure and safeguard the PII it collected, generated, and stored to prevent disclosure of the information, and to guard the information from theft.

76. Defendant's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

77. Defendant also owed a duty of care to Plaintiff and the Class members to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that its systems and networks and the personnel responsible for them adequately protected its customers' PII.

78. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between it and its patients. This duty is recognized by law, including but not limited to HIPAA and the FTCA. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the Class members that would arise from a data breach.

79. Defendant's duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendant is required to "reasonably safeguard protected health information from any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[35] The data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

80. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

81. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because it is bound by, and has committed to comply with, industry standards for the protection of confidential PII.

82. Defendant occupied a special relationship with Plaintiff and the Class, who were Defendant's patients.

[35] C.F.R. § 164.530(c)(1).

83. Defendant breached its common law and other duties by failing to use reasonable measures to protect patients' PII.

84. Defendant failed to disclose material information to Plaintiff and the Class at the time they provided their PII, *i.e.*, that Defendant did not have sufficient security or mechanisms to protect PII, and, in fact, represented that it employed adequate security measures.

85. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' PII;

b. failing to appropriately train its staff about the dangers of phishing attacks;

c. failing to adequately monitor the security of its network and systems;

d. actively and knowingly misrepresenting or omitting disclosure of material information to Plaintiff and the Class at the time they provided such PII that Defendant did not have sufficient security or mechanisms to protect PII;

e. allowing unauthorized access to Plaintiff's and Class members' PII; and

f. failing to recognize in a timely manner that Plaintiff's and other Class members' PII had been compromised.

86. It was foreseeable that Defendant's failure to use reasonable measures to protect PII would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the Class members were reasonably foreseeable.

87. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the Class members:

a. ongoing, imminent, impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;

b. actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;

c. loss of the confidentiality of the stolen confidential data;

d. the illegal sale of the compromised data on the black market;

e. expenses and/or time spent on credit monitoring and identity theft insurance;

f. time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts;

g. decreased credit scores and ratings;

h. lost work time;

i. and other economic harm.

88. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring that Defendant's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II
NEGLIGENCE PER SE

89. Plaintiff incorporates the above allegations by reference.

90. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiff's and Class members' PII.

91. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' PII.

92. Defendant breached its duties to Plaintiff and Class members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d et. seq.) by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Class members' PII.

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

94. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

95. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their PII.

96. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
NEGLIGENT MISREPRESENTATION

97. Plaintiff incorporates the above allegations by reference.

98. Defendant owed Plaintiff and Class members a duty and occupied a special relationship with Plaintiff and Class members, as Defendant's patients, and as described above.

99. Defendant negligently prepared information and misrepresented material facts, pertaining to the provision of health care services, to Plaintiff and Class members by

representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft.

100. Healthcare providers have received multiple warnings of their vulnerability to cyber attacks, and Defendant was already aware it had been targeted in a phone phishing scam. Because Defendant was aware of the susceptibility of healthcare providers to cyber attacks and also its own heavy reliance on email for sharing confidential information and other security vulnerabilities, Defendant either knew or should have known its representations were untrue.

101. In reasonable and justifiable reliance upon these misrepresentations, Plaintiff and Class members purchased healthcare services from Defendant.

102. Had Plaintiff and Class members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Class members' PII, they would not have purchased healthcare services benefits from Defendant, and would not have entrusted their PII to Defendant.

103. As a direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiff and Class members have suffered the injuries alleged above.

COUNT IV
VIOLATIONS OF MICHIGAN'S DATA BREACH PROMPT NOTIFICATION LAW (MICH. COMP. LAWS ANN. § 445.72(1), *et seq.*)

104. Plaintiff incorporates the above allegations by reference.

105. Defendant is required to accurately notify Plaintiff and Class Members if it discovers a security breach, or receives 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).

106. Defendant is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

107. Plaintiff and Class Members' Personal Information (e.g. Social Security numbers) includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

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

109. Defendant has stated it was aware of a security breach in August when it hired a third-party cyber security firm to investigate a phishing attack. However, Defendant did not notify Plaintiff and the Class until February, approximately six months after it first learned of a security breach.

110. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Class Members suffered damages.

111. Plaintiff and Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including, but not limited to, a civil fine of up to $250 for each violation.

COUNT V
UNJUST ENRICHMENT

112. Plaintiff incorporates the above allegations by reference.

113. Plaintiff and Class members conferred a monetary benefit on Defendant in the form of monies paid for the purchase of health services from Defendant prior to and during the period of the data breach.

114. Defendant appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and the Class members.

115. The monies paid for the purchase of health services by Plaintiff and the Class members to Defendant during the period of the data breach were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and the Class members.

116. Defendant failed to provide reasonable security, safeguards, and protection for the PII of Plaintiff and Class members and, as a result, Plaintiff and Class members overpaid Defendant for the services purchased.

117. Had Plaintiff and the Class known that Defendant would not adequately protect their PII, they would not have elected to purchase health care services from Defendant or would have paid less for the same services.

118. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class members, because Plaintiff and Class members paid for adequate safeguards and security measures to protect their PII that Defendant did not provide.

119. Plaintiff and the Class have conferred directly upon Defendant an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class members.

120. The economic benefit, including the monies paid and the overcharges and profits derived by Defendant and paid by Plaintiff and the Class members, is a direct and proximate result of Defendant's unlawful practices as set forth in this Complaint.

121. The financial benefits derived by Defendant rightfully belong to Plaintiff and the Class members.

122. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and the Class.

123. Plaintiff and the Class have no adequate remedy at law.

COUNT VI
BREACH OF IMPLIED CONTRACT

124. Plaintiff incorporates the above allegations by reference.

125. When Plaintiff and the Class members provided their PII to Defendant in order to purchase services from them, Plaintiff and the Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to notify Plaintiff and the Class members in a timely and accurate manner that their data had been breached and compromised.

126. Plaintiff and the Class members would not have provided and entrusted their financial, health, and other PII to Defendant in order to purchase healthcare from Defendant in the absence of the implied contract between them and Defendant.

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

128. Defendant breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect the health, financial, and other PII of Plaintiff and the Class members and by failing to provide timely and accurate notice to them that their PII was compromised in and as a result of the Breach.

COUNT VII
BREACH OF CONTRACT

129. Plaintiff incorporates the above allegations by reference.

130. Defendant has a contractual obligation to maintain the security of its patients' personal, health, and financial information, which Defendant recognizes in its Notice of Privacy Practices where it addresses the consumers' "protected health information."

131. Defendant also specifically promised that it would notify the client "at the time of data collection or transfer if your data will be shared with a third party and you will always have the option of not permitting the transfer. If you do not wish to allow your data to be shared, you can choose not to provide that information or use a particular service."[36]

132. Defendant breached these contractual obligations by failing to safeguard and protect the PII of Plaintiff and the Class members, including through the dissemination of PII through unsecured email and through the unauthorized disclosure of PII, including personal, health, and financial information, to unauthorized third parties.

133. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of the breaches of the contracts between Defendant and Plaintiff and the Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment against Defendant as follows:

A. Certifying this action as a class action, with a Class as defined above;

[36] Munson Healthcare, Website Privacy Statement, available at: https://www.munsonhealthcare.org/about-the-system/website-privacy-policy# (last visited April 22, 2020).

B. Awarding compensatory damages to redress the harm caused to Plaintiff and the Class members in the form of, *inter alia*, overpayment, direct theft, identity theft, loss of unencumbered use of existing passwords, loss of passwords, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, and other harm. Plaintiff and the Class members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court;

C. Ordering injunctive relief including, without limitation, requiring Defendant to (i) provide credit monitoring for all Class members, (ii) provide identity theft insurance, (iii) institute security protocols in compliance with the appropriate standards; and (iv) require Defendant to submit to periodic compliance audits by a third party regarding the security of consumers' personal identifying information in its possession, custody and control;

D. Awarding Plaintiff and the Class interest, costs and attorneys' fees; and

E. Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Pursuant to Federal Rule of Civil Procedure Rule 38, Plaintiff demands a jury trial.

Dated: April 30, 2020

Respectfully submitted,

/s/Jesse L. Young
Jesse L. Young (P72614)
KREIS ENDERLE, P.C.
8225 Moorsbridge
P.O. Box 4010
Kalamazoo, MI 49003
Tel: (269) 321-2311
jyoung@kreisenderle.com

Nicholas A. Migliaccio
Jason S. Rathod

MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Jason P. Sultzer
THE SULTZER LAW GROUP P.C.
85 Civic Center Plaza, Suite 200
Poughkeepsie, New York 12601
Tel: (845) 483-7100
Fax: (888) 749-7747
sultzerj@thesultzerlawgroup.com

Counsel for Plaintiff and the Class