☐ YES ☒ NO

EXHIBITS

CASE NO. 22CH7101

DATE: 7-22-22

CASE TYPE: Class Action

PAGE COUNT: 28

CASE NOTE

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

QIXIN CHEN and BEICHEN SHI, Individually, and on Behalf of All Others Similarly Situated,	)	Case No. 2022CH07101
Plaintiffs,	)	
v.	)	**JURY TRIAL DEMANDED**
MICHIGAN AVENUE IMMEDIATE CARE, S.C.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Qixin Chen and Beichen Shi, ("Plaintiffs"), through their undersigned counsel, bring this action against Michigan Avenue Immediate Care, S.C. ("MAIC" or "Defendant") pursuant to the investigation of her attorneys, personal knowledge as to themselves and their own acts and otherwise upon information and belief, and allege as follows:

INTRODUCTION

1. Michigan Avenue Immediate Care is an urgent care center located in Chicago, Illinois.

2. On or about June 24, 2022, MAIC announced publicly that on May 1, 2022, it had been the recipient of a hack and exfiltration of sensitive personal information ("SPI") involving approximately 144,104 of its patients (the "Data Breach").

3. However, at least one online source is reporting that the Data Breach may have occurred as early as December 2021 and was done by actors referring to themselves as "Targetware

Team," who were also responsible for the recent data breach involving The Unified Government of Wyandotte County and Kansas City.[1]

4. MAIC reported that this SPI included names, addresses, dates of birth, Social Security numbers, driver's license numbers, treatment information, and/or health insurance information.[2]

5. Plaintiffs and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

6. The information stolen in cyber-attacks allows the modern thief to assume your identity when carrying out criminal acts such as:

- Using your credit history.
- Making financial transactions on your behalf, including opening credit accounts in your name.
- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Committing illegal acts which, in turn, incriminate you.

7. Plaintiffs' and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiffs and Class members.

8. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of

---

[1] *See* https://www.databreaches.net/immediate-care-facility-in-chicago-hacked-in-december-do-patients-know/ (last accessed July 22, 2022)

[2] *See* https://www.michiganavenueimmediatecare.org/notice-of-data-incident/ (last accessed July 12, 2022)

personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* (the "ICFA"); and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendant because it operates within the State of Illinois and derives substantial revenue from its operations, and otherwise seeks the legal benefits and protections afforded by the State of Illinois.

12. Venue is proper pursuant to 735 ILCS 5/2-101 because a substantial part of the events or omissions giving rise to these claims occurred in this County. Specifically, Plaintiffs and Defendant are domiciled in or residents of Cook County.

PARTIES

13. Plaintiff Qixin Chen is a natural person residing in Chicago, Illinois. On or about July 1, 2022, Plaintiff Chen was informed via letter dated June 24, 2022 that she had been a victim of the Data Breach.

14. Plaintiff Beichen Shi is a natural person residing in Chicago, Illinois. On or about July 1, 2022, Plaintiff Shi was informed via letter dated June 24, 2022 that he had been a victim of the Data Breach.

15. Defendant Michigan Avenue Immediate Care, S.C. is an Illinois corporation with its principal place of business at 180 N. Michigan Ave., Suite 1605, Chicago, Illinois.

FACTUAL ALLEGATIONS

16. Defendant is an urgent care clinic located on Michigan Avenue in Chicago, Illinois. Defendant sees at thousands of patients per year at its offices.

17. In the ordinary course of doing business with Defendant, patients and prospective patients are required to provide Defendant with SPI such as:

a. Contact and account information, such as name, usernames, passwords, address, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, driver's license number, and signature;

c. Demographic information, such as age, gender, and date of birth;

d. Payment information, such as credit card, debit card, and/or bank account number; and

e. Medical history as self-reported by patients, or medical history as transmitted from other healthcare providers.

18. Defendant also automatically collects the following SPI from its patients, including medical and diagnosis history from its own physicians; treatment information; and prescription information, among other types of information.

19. Defendant represents on its website: "We are committed to protecting your privacy and developing technology that gives you the most powerful and safe online experience."[3]

20. Defendant also prominent links to a page that describes itself as "HIPAA Notice of Privacy Practices."[4]

21. The HIPAA Notice of Privacy Practices "describes how we many use and disclose your protected health information (PHI) to carry out treatment, payment or healthcare operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your PHI. Protected health information is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services"[5]

22. The HIPAA Notice of Privacy Practices states that PHI (which is includes information previously referenced as Plaintiffs' and Class Members' SPI) may be disclosed "by our physicians, office staff and others outside of our office that are involved in your care and treatment for the purposes of providing health care services to you. Your PHI may also be used and disclosed to obtain payment for services provided to you and to support the operation of our practice."[6]

---

[3] https://www.michiganavenueprimarycare.com/your-privacy (last accessed July 13, 2022)
[4] *See* https://sa1s3.patientpop.com/assets/docs/370629.pdf (last accessed July 13, 2022)
[5] *Id.*
[6] *Id.*

23. Defendant then lists a few other scenarios by which PHI could be disclosed, but states that "Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described below."[7]

24. Defendant's Data Breach was not enumerated on its website as a basis for its disclosure of SPI or PHI.

25. On or about July 1, 2022, Defendant announced publicly that on May 1, 2022, it became aware of a hack and exfiltration of sensitive personal information involving its patients.[8]

26. However, at least one online source is reporting that the breach may have occurred as early as December 2021 and continued through May 2022. The source states:

> On Monday, DataBreaches.net was contacted by an individual who claimed that Michigan Avenue Immediate Care had been hacked.
>
> "Stealed more that 580 GB personal information about ~43.000 patients including SSN , Proof ID and lab analyses , TEMPUS Covid information and more info," the person wrote, using a protonmail account."
>
> A single 13-page file with a named patient's registration form for Michigan Avenue Immediate Care (MAIC) was attached. The form contained demographic information about the patient with their name, date of birth, address, telephone number, Social Security number, health insurance information, and medical history including lifestyle factors was provided. That file also included a photocopy of the patient's driver's license and an April, 2022 date for follow up at Michigan Avenue Primary Care.[9]

27. Further, DataBreaches.net states

> When asked for information about when the attack occurred, the threat actors replied (as in the original):

---

[7] *Id.*

[8] https://www.hipaajournal.com/data-breaches-reported-by-university-pediatric-dentistry-orthonebraska-michigan-avenue-immediate-care/ (last accessed July 22, 2022)

[9] https://www.databreaches.net/immediate-care-facility-in-chicago-hacked-in-december-do-patients-know/ (last accessed July 22, 2022)

> "We has break his servers on december 2021 . We continued uploading his data until to 10 May . We collected data from Yosi System, Docman , Tempus Covid results and more another info . We demanded not big price for confidential about this breach, but he only delay time, not paying."

Of note, they also informed DataBreaches that they had not encrypted any files.[10]

28. This reporting strongly implies that MAIC knew or should have known of the Data Breach earlier than May 1, 2022, but did not act on it until at least May.

29. DataBreaches.net also states that Targetware Team informed them that the information stolen from MAIC, which Targetware Team described as having "very weak computer security", has all been sold.[11]

30. While the Data Breach was reported in trade journals at the time, there appears to to have been no wide-scale press release as local press, such as WTTW, WBEZ, and the Chicago Tribune did not report on it at the time.

31. Plaintiffs' notification letter is dated June 24, 2022, indicating that Defendant waited approximately eight weeks to directly notify affected persons even though it knew of the Data Breach months earlier.

32. MAIC reported to the U.S. Department of Health and Human Services that the total number of Individuals Affected was approximately 144,104.[12]

33. As a result, Plaintiffs' and class members' SPI was in the hands of hackers for approximately as much as seven months before Defendant began notifying them of the Data Breach.

---

[10] https://www.databreaches.net/immediate-care-facility-in-chicago-hacked-in-december-do-patients-know/ (last accessed July 22, 2022)

[11] *Id.*

[12] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed July 22, 2022)

34. Defendant has been extremely vague on its response to the Data Breach, stating only that "We continue to implement appropriate safeguards to protect patient information."

35. As of this writing, Defendant has offered no concrete information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

36. Defendant has also stated that it is offering credit monitoring for one year to impacted individuals.

37. However, this response is entirely inadequate to Plaintiffs and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

38. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

39. Plaintiffs and Class members provided their SPI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

40. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the cellular communications services industry preceding the date of the breach.

41. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

42. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc

on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[13] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[14]

43. The SPI of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiffs and members of the Class, including Social Security numbers, driver license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class a result of a breach.

45. Plaintiffs and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI.

46. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiffs and members of the Class.

47. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need

---

[13] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, (last accessed July 13, 2022)

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

for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

49. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

52. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

53. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

54. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

55. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

56. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

57. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15]

58. Social Security numbers, for example, are among the worst kind of personal

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last accessed July 13, 2022).

information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

59. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

60. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

61. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is

---

[16] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 13, 2022).

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed July 13, 2022)

> especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[18]

62. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiffs and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Class. Stolen personal data of Plaintiffs and members of the Classes represents essentially one-stop shopping for identity thieves.

63. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

64. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [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.[19]

65. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable

---

[18] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 13, 2022)

[19] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last accessed July 13, 2022)

commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiffs and members of the Class has a high value on both legitimate and black markets.

66. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

67. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

---

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 15, 2022)

70. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits."[21]

71. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits)

FACTS SPECIFIC TO PLAINTIFFS

72. On or about July 1, 2022, Plaintiffs were notified via letter from Defendant dated June 24, 2022 that Plaintiffs' SPI had been taken as part of the Data Breach.

73. Plaintiff Chen has been a patient of Defendant several times between November 9, 2021 and June 27, 2022. Plaintiff Shi was a patient of Defendant on December 29, 2021.

74. Had Plaintiffs known that their SPI would not have been adequately protected by Defendant, they would not have used Defendant's services or they would have insisted that their SPI not be stored in Defendant's system.

75. Since the time of the Data Breach, Plaintiffs have received numerous calls from various scammers attempting to get her to sign up for medical benefits and other scams. This activity indicates that their information has been placed into the hands of hackers and has already

[21] https://www.identityguard.com/news/kids-targeted-identity-theft (last accessed July 22, 2022)

been sold throughout the dark web.

76. Additionally, Plaintiffs are aware of no other source from which the theft of their SPI could have come. They regularly take steps to safeguard their own SPI in their own control.

CLASS ACTION ALLEGATIONS

77. This action satisfies the prerequisites for maintenance as a class action pursuant to 735 ILCS 5/2-801 *et seq.*, as set forth below.

78. Class Definition. Plaintiffs bring this action individually and on behalf of the following class of similarly situated persons (the "Class"), of which Plaintiffs are a member:

> All persons whose information was accessed as a result of the Data Breach that is the subject of this Complaint.

Excluded from the class are Defendant's officers, directors or employees, the presiding judge, Class counsel and any member of their immediate families. Plaintiffs hereby reserve the right to amend the class definition based on discovery and the proofs at trial.

79. Numerosity. The members of the Class are so numerous that joinder of all members would be impracticable. The precise number of Class members is currently understood to be 144,104. Potential Class members may be notified of the pendency of this action by first class mail, electronic mail, and/or published notice as appropriate and as determined by the court.

80. Commonality. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, *inter alia*, the following:

> (i) Whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act by failing to maintain adequate security for Plaintiffs' and Class Members' SPI;
>
> (ii) Whether Defendant violated the Illinois Consumer Fraud and Deceptive Business Practices Act by failing to timely notify Plaintiffs and Class Members of the Data Breach;

(iii) Whether Defendant breached its warranty to Plaintiffs and the Class by failing to maintain adequate security for Plaintiffs' and Class Members' SPI; and

(iv) Whether Defendant was unjustly enriched by Plaintiffs and the Class by failing to maintain adequate security for Plaintiffs' and Class Members' SPI.

81. Typicality. The claims of Plaintiffs are typical of the claims of the members of the Class because, *inter alia*, all Class members were injured through the uniform misconduct described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all members of the Class.

82. Adequacy. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have retained highly competent counsel and experienced class action attorneys to represent their interests and that of the Class. Plaintiffs and their counsel have the necessary financial resources to adequately and vigorously litigate this class action. Plaintiffs have no adverse or antagonistic interests to those of the Class. Plaintiffs are willing and prepared to serve the Court and the Class members in a representative capacity with all of the obligations and duties material thereto and is determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

83. Appropriateness. A class action is an appropriate method for the fair and efficient adjudication of this controversy. The common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class. Also, the likelihood that individual members of the Class will prosecute separate actions is remote due to the extensive time and considerable expense necessary to conduct such litigation, especially in view of the relatively modest amount of monetary relief at issue for individual Class members.

84. A class action will cause an orderly and expeditious administration of the claims of the Class. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

85. Plaintiffs do not anticipate any undue difficulty in the management of this litigation.

86. Plaintiffs adopt and incorporate by reference all prior paragraphs of this Complaint as if fully set forth herein.

FIRST CLAIM FOR RELIEF
(Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 ILCS 505/1 *et seq.*)

87. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 85.

88. Plaintiffs are "consumers" as that term is defined in 815 ILCS 505/1(e).

89. Defendant is engaged in "trade" or "commerce", including the provision of services, as those terms are defined under 815 ILCS 5051(f).

90. Defendant engages in the "sale" of services as defined in 815 ILCS 505/1(b).

91. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ICFA) in violation of the ICFA, including but not limited to the following:

a. Failing to maintain sufficient security to keep Plaintiffs' and Class Members' SPI from being hacked and stolen; and

b. Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Class Members' SPI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

92. In addition, Defendant's failure to disclose that its computer systems were not well-protected and that Plaintiffs' and Class Members' SPI was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and Class Members; and (b) defeat Plaintiffs' and Class Members' ordinary, foreseeable and reasonable expectations concerning the security of their SPI on Defendants' servers.

93. Defendant intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with its offering of services and incorporating Plaintiffs' and Class Members' SPI on its servers, in violation of the ICFA.

94. Defendant also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiffs' and Class Members' SPI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

95. Defendant's wrongful acts and practices occurred within the ordinary course of trade or commerce.

96. Defendant's wrongful acts and practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to Plaintiffs and Class Members and were repeated continuously before and after Defendant obtained SPI and other information from Plaintiffs and Class Members. Plaintiffs and Class Members were adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

97. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and Class Members of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/45, *et. seq.*, which provides:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

98. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

99. As a result of Defendant's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have allowed their SPI – the value over which Plaintiffs and Class Members no longer have control – to be provided to Defendant if they had been told or knew that Defendant failed to maintain sufficient security to keep such data from being hacked and taken by others.

100. Defendant's unfair and/or deceptive conduct proximately caused Plaintiffs' and Class Members' injuries because, had Defendant maintained customer SPI with adequate security, Plaintiffs and Class Members would not have lost it.

101. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made from Defendant that Plaintiffs and Class Members would have never made had they known of Defendant's careless approach to cybersecurity; lost control over the value of SPI; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen SPI, entitling them to damages in an amount to be proven at trial.

102. Pursuant to 815 ILCS 505/10a(a), Plaintiffs and Class Members seek actual and compensatory damages, injunctive relief, and court costs and reasonable attorneys' fees as a result of Defendant's violations of the ICFA.

Prayer for Relief

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' SPI;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database (if, in fact, it does so);

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying

information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party

assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For pre- and postjudgment interest on all amounts awarded; and

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

SECOND CLAIM FOR RELIEF
Breach of Implied Contract

103. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 85.

104. When Plaintiffs and Class Members provided their SPI to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

105. Defendant solicited and invited Plaintiffs and Class Members to provide their SPI as part of Defendant's regular business practices and as essential to the services transactions entered into between Defendant on the one hand and Plaintiffs and Class Members on the other. This conduct thus created implied contracts between Plaintiffs and Class Members on the one hand, and Defendant on the other hand. Plaintiffs and Class Members accepted Defendant's offers by providing their SPI to Defendant in connection with their purchases from Defendant.

106. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

107. Defendant's implied promise to safeguard Plaintiffs' and Class Members' SPI is evidenced by a duty to protect and safeguard SPI that Defendant required Plaintiffs and Class Members to provide as a condition of entering into consumer transactions with Defendant.

108. Plaintiffs and Class Members paid money to Defendant to purchase services from Defendant. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of funds received as a result of the purchases to obtain adequate data security. Defendant failed to do so.

109. Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from patients' continued use of Defendant's services—that Defendant would adequately safeguard SPI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Class Members.

110. Plaintiffs and Class Members value data security and would not have provided their SPI to Defendant in the absence of Defendant's implied promise to keep the SPI reasonably secure.

111. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

112. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

113. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

114. Plaintiffs and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

115. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiffs and Nationwide Class members.

Prayer for Relief

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' SPI;

C. For an award of damages, including actual, nominal, compensatory, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

E. For pre- and postjudgment interest on all amounts awarded; and

F. Such other and further relief as this Court may deem just and proper.

THIRD CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative

116. Plaintiffs hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 85.

117. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

118. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefited from the receipt of Plaintiffs' and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

119. The benefits given by Plaintiffs and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

120. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount to be determined at trial.

121. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

122. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

Prayer for Relief

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and the following:

G. For an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

H. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' SPI;

I. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

J. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

K. For pre- and postjudgment interest on all amounts awarded; and

L. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

NOTICE TO ILLINOIS ATTORNEY GENERAL OF ACTION

Pursuant to 815 ILCS 505/10a (d), a copy of this Complaint has been mailed to the Illinois Attorney General with the filing of this Complaint.

DATED: July 22, 2022

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*
Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Attorney No. 38819
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiffs and the Putative Class

whafhch57089