UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

KATHLEEN TUCKER, on behalf of themselves and all others similarly situated, Plaintiff, v. **MARIETTA AREA HEALTH CARE INC. D/B/A MEMORIAL HEALTH SYSTEM,** Defendant.	Case No. Judge **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kathleen Tucker, individually and on behalf of all others similarly situated, brings this action against Defendant Marietta Area Health Care Inc. d/b/a Memorial Health System (hereinafter known as "Memorial Health" or "Defendant"), an Ohio corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Memorial Health's network that resulted in unauthorized access to customer data. As a result of the Data Breach, Plaintiff and approximately 216,478 Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/e7861ebb-6f43-4fe7-9619-25762e3be35d.shtml (Last visited Jan. 19, 2022).

2. In addition, Plaintiff and Class Members' sensitive personal information—which was entrusted to Memorial Health, its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, "PII"), and medical and treatment information ("PHI"), The PII and PHI that Defendant Memorial Health collected and maintained will be collectively referred to as the "Private Information."

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

6. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Memorial Health collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, and (iii) breach of implied contract; and (iv) unjust enrichment.

THE PARTIES

13. Plaintiff Kathleen Tucker is a natural person, resident and a citizen of the State of West Virginia. She has lived in West Virginia since 1979 and has no intention of moving to a different state in the immediate future. She is registered to vote in West Virginia as well. Plaintiff Tucker is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Tucker's PII and PHI and owed her a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff Tucker would not have entrusted her PII and PHI to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Tucker's PII and PHI was compromised and disclosed as a result of Defendant's inadequate data security and the Data Breach.

JURISDICTION AND VENUE

14. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiff (and many members of the class) and Defendant are citizens of different states.

15. This Court has general personal jurisdiction over Memorial Health because Memorial's principal place of business is, and does regularly conduct business, in Marietta, Ohio.

16. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Memorial Health conducts substantial business in this District.

DEFENDANT'S BUSINESS

17. Memorial Health provides comprehensive medical care throughout the Marietta and surrounding region.

18. Defendant Memorial Health "employs over 2,700 employees, including 325 providers representing 64 clinics."[2] Memorial Health represents that it "strive[s] to deliver quality, affordable care with an additional focus on medical and community service."[3]

19. Defendant Memorial Health claims it "is dedicated to providing you with healthcare information and referral services of the highest quality, whole at the same time protecting your privacy."[4]

20. Defendant Memorial Health further claims it is "very concerned with the security of your personally identifiable information and take[s] great care in providing secure transmission of your information from your computer to our services."[5] Defendant also states that "[o]nce we receive your information, we take appropriate steps that we believe are reasonable to protect the security of your data on our system."[6]

21. On information and belief, in the ordinary course of rendering healthcare care services, Memorial Health requires its patients and customers to provide sensitive personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;

[2] Mission and Vison, Memorial Health, https://mhsystem.org/missionandvision (Last visited Jan. 19, 2022).
[3] *Id*.
[4] Web Site Privacy Notice, Memorial Health, https://mhsystem.org/websiteprivacy (Last visited Jan. 19, 2022).
[5] *Id*.
[6] *Id*.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.