UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

LEO THORBECKE and MARJORITA DEAN, individually and on behalf of all others similarly situated, Plaintiff, v. MCG HEALTH, LLC, a Washington limited liability company, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Leo Thorbecke and Marjorita Dean ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action against Defendant MCG Health, LLC ("MCG Health" or "Defendant") and allege as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28

U.S.C. § 1367 because they form part of the same case or controversy as the claims within the Court's original jurisdiction.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiffs' claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

PARTIES

4. Plaintiff Leo Thorbecke is a resident and citizen of Indiana.

5. Plaintiff Marjorita Dean is a resident and citizen of Ohio.

6. Defendant MCG Health, LLC is a Washington limited liability company with its principal place of business in Seattle, Washington.

7. Defendant MCG Health is a division of Hearst Corporation, a Delaware corporation.

FACTUAL ALLEGATIONS

I. MCG Health

8. Defendant MCG Health is a Seattle-based software company that "provides patient care guidelines to health care providers and health plans."[1]

9. A majority of U.S. health plans and nearly 2,600 hospitals utilize Defendant's software and are Defendant's customers.

[1] https://www.businesswire.com/news/home/20220610005006/en/Notice-Provided-to-Individuals-Regarding-MCG-Data-Security-Incident

10. Patients and members of Defendant's customers, like Plaintiffs and Class members, provided certain Personal Identifying Information ("PII") and Protected Health Information ("PHI") to their healthcare providers which is required as a condition of medical treatment. Plaintiffs' and Class members' PII and PHI was then provided to Defendant.

The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.[2]

11. As a large technology company with an acute interest in maintaining the confidentiality of the PII and PHI entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII and PHI in its possession.

12. Defendant represents to patients and members and the public that it possesses robust security features to protect PII and PHI.

II. The Data Breach

13. On June 10, 2022, Defendant announced in a press release that it was investigating a data security incident that it had initially discovered on March 25, 2022. Defendant's investigation included assistance of a forensic investigation firm.[3]

14. The investigation determined that "an unauthorized party previously obtained personal information about some patients and members of certain MCG customers. The affected patient or member data included some or all of the following data elements: names, Social

[2] *Id.*
[3] *Id.*

Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender."[4]

15. On or about April 22, 2022, MCG notified its affected customers (i.e., healthcare systems) of the breach. In turn, MCG customers began notifying their patients in June 2022.

16. Defendant sent a letter to Plaintiffs Dean and Thorbecke dated June 10, 2022, notifying them of the breach. *See* Exhibit A and Exhibit B.[5]

17. Defendant's letter also offered two years of free identity protection services to affected patients and members.

18. Defendant did not state why it was unable to detect the unauthorized individuals accessing Defendant's servers.

19. Defendant did not state why it waited for nearly three months before notifying affected patients and members.

20. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

III. Injuries to Plaintiffs and the Class

21. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs' PII and PHI, Plaintiffs and the Class have been damaged.

22. Plaintiffs and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages,

---

[4] *Id.*

[5] *See also* https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf.

including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

23. In addition to the irreparable damage that may result from the theft of PII and PHI, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

24. In addition to fraudulent charges and damage to their credit, Plaintiffs and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

25. Additionally, Plaintiffs and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII and PHI is used, the diminution in the value and/or use of their PII and PHI entrusted to Defendant, and loss of privacy.

---

[6] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

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.