

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

**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

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

3 2. This Court has general personal jurisdiction over Defendant because Defendant is
4 a resident and citizen of this district, Defendant conducts substantial business in this district, and
5 the events giving rise to Plaintiffs' claims arise out of Defendant's contacts with this district.
6

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

10 **PARTIES**

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

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

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

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

16 **FACTUAL ALLEGATIONS**

17 **I. MCG Health**

18 8. Defendant MCG Health is a Seattle-based software company that "provides patient
19 care guidelines to health care providers and health plans."¹
20

21 9. A majority of U.S. health plans and nearly 2,600 hospitals utilize Defendant's
22 software and are Defendant's customers.
23

24
25
26

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

1 10. Patients and members of Defendant’s customers, like Plaintiffs and Class
2 members, provided certain Personal Identifying Information (“PII”) and Protected Health
3 Information (“PHI”) to their healthcare providers which is required as a condition of medical
4 treatment. Plaintiffs’ and Class members’ PII and PHI was then provided to Defendant.
5

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

9 11. As a large technology company with an acute interest in maintaining the
10 confidentiality of the PII and PHI entrusted to it, Defendant is well-aware of the numerous data
11 breaches that have occurred throughout the United States and its responsibility for safeguarding
12 PII and PHI in its possession.
13

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

16 **II. The Data Breach**

17 13. On June 10, 2022, Defendant announced in a press release that it was investigating
18 a data security incident that it had initially discovered on March 25, 2022. Defendant’s
19 investigation included assistance of a forensic investigation firm.³
20

21 14. The investigation determined that “an unauthorized party previously obtained
22 personal information about some patients and members of certain MCG customers. The affected
23 patient or member data included some or all of the following data elements: names, Social
24

25 ² *Id.*

26 ³ *Id.*

1 Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of
2 birth and gender.”⁴

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

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

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

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

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

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

16
17
18 **III. Injuries to Plaintiffs and the Class**

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

21 22. Plaintiffs and the Class have been placed at a substantial risk of harm in the form
22 of credit fraud or identity theft and have incurred and will likely incur additional damages,
23

24
25 ⁴ *Id.*

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

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

3 23. In addition to the irreparable damage that may result from the theft of PII and PHI,
4 identity theft victims must spend numerous hours and their own money repairing the impacts
5 caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice
6 Statistics found that identity theft victims "reported spending an average of about 7 hours clearing
7 up the issues" and resolving the consequences of fraud in 2014.⁶

8
9 24. In addition to fraudulent charges and damage to their credit, Plaintiffs and the
10 Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent
11 or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and
12 identity theft prevention services; (d) attempting to withdraw funds linked to compromised,
13 frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f)
14 communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic
15 billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account
16 information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late
17 fees and declined payment penalties as a result of failed automatic payments.

18
19 25. Additionally, Plaintiffs and the Class have suffered or are at increased risk of
20 suffering from, *inter alia*, the loss of the opportunity to control how their PII and PHI is used, the
21 diminution in the value and/or use of their PII and PHI entrusted to Defendant, and loss of
22 privacy.
23

24
25
26

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

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.