UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

LINDA BOOTH, MARY NAPIER, and CANDACE DAUGHERTY on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

MCG Health, LLC,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Linda Booth, Mary Napier, and Candace Daugherty, individually and on behalf of the proposed class defined below, bring this action against Defendant MCG Health, LLC ("MCG") allege as follows:

## I. SUMMARY OF THE ACTION

1. This action arises out of MCG's failure to secure the highly sensitive personal information of its patients. Around February 25 to 26, 2020, an unauthorized party or parties accessed MCG's computer systems and exfiltrated patient files (the "Data Breach"). MCG did not learn of the breach until more than two years later, on March 25, 2022 and determined that the exfiltrated files contained patient names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and genders. Over 1,100,000 patients' personally identifiable information ("PII") and personal health information ("PHI") was compromised in the attack.

2. Even after MCG learned of the hack on March 25, 2022, it did not notify affected patients of the attack until June 10, 2022. During this time, those patients remained unaware that

their information had been compromised. The personal information remains in the possession of the unauthorized party or parties.

3. As a result of MCG's data security failures, Plaintiffs and Class members confront a significant threat of identity theft and other harm—imminently and for years to come. Plaintiffs by this action seek damages together with injunctive relief to remediate MCG's deficient cybersecurity protocols and provide identity theft insurance (or the money needed to secure those services) to protect them and the other breach victims from identity theft and fraud.

## II. PARTIES

***Plaintiff Linda Booth***

4. Plaintiff Linda Booth is a citizen and resident of Santa Fe, New Mexico.

5. Plaintiff Booth received a letter dated June 10, 2022 from MCG notifying her of the Data Breach and stating that it "affects certain of your personal information." The letter stated that an unauthorized party "previously obtained certain of your personal information that matched data stored on MCG's systems." Affected information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

***Plaintiff Mary Napier***

6. Plaintiff Mary Napier is a citizen and resident of Rogers, Kentucky

7. Plaintiff Napier received a letter dated June 10, 2022, from MCG notifying her of the Data Breach and stating that it "affects certain of your personal information." The letter stated that an unauthorized party "previously obtained certain of your personal information that matched data stored on MCG's systems." Affected information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

***Plaintiff Candace Daugherty***

8. Plaintiff Candace Daugherty is a citizen and resident of Vancleave, Mississippi.

9. Plaintiff Daugherty received a letter dated June 10, 2022, from MCG notifying her of the Data Breach and stating that it "affects certain of your personal information." The letter stated that an unauthorized party "previously obtained certain of your personal information that matched data

stored on MCG's systems." Affected information includes names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

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

## III. JURISDICTION AND VENUE

11. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of Class members exceeds $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) MCG Health and Class members are domiciled in different states.

12. This Court has personal jurisdiction over Defendant MCG health because its principal place of business is within this District, and it has sufficient minimum contacts in Washington to render the exercise of jurisdiction by this Court proper and necessary.

13. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

## IV. FACTUAL ALLEGATIONS

### MCG Health and the Data Breach

14. MCG is a HIPPA business associate that provides care guidelines to healthcare providers and health plans. A HIPPA business associate is an entity that provides services to a HIPPA covered entity (i.e., a hospital) that involves the disclosure of personal health information. HIPPA business associates are often software companies that have access to large quantities of personal health information.

15. MCG develops and institutes software and evidence-based care guidelines to assist healthcare payers, providers, and government healthcare agencies in making decisions related to patient care.

16. MCG Health is part of the Hearst Health network. MCG states that a "majority of U.S. health plans and nearly 2,600 hospitals" use their services.

17. For the past 30 years, MCG has worked with state, regional, and federal government healthcare agencies and government contractors, in government administered healthcare programs.

18. As part of its business operations, MCG collects from Plaintiffs and Class Members or the healthcare networks, providers, and plans that they use, information including names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and genders.

19. On March 25, 2022, MCG discovered that an unauthorized party accessed patient and member data stored on MCG's systems. MCG states that "there is evidence to suggest the data may have been acquired by an unauthorized party on or around February 25-26, 2020." MCG, however, also asserts that it is uncertain as to when the data was first acquired by unauthorized parties.

20. Around June 10, 2022, over two years after the hack occurred and almost three months after discovering the breach, MCG informed its patients and members of the data breach and advised them to take protective measures. The letter stated that MCG experienced suspicious activity on its computer network and an unauthorized party or parties obtained personal information that matched data stored in MCG's systems. The letter informed victims of the breach that the following information had been compromised: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

21. Plaintiffs suffer stress and anxiety as a result of the Data Breach and from the loss of their privacy.

22. Plaintiffs also suffered injury in the form of damage to and diminution in the value of their confidential personal information—a form of property that Plaintiffs entrusted to Defendant, and which was compromised as a result of the Data Breach it failed to prevent.

23. Plaintiffs suffer a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from their personal information being placed in the hands of unauthorized third parties.

24. Plaintiffs have a continuing interest in ensuring that their personal information is protected and safeguarded from future breaches.

**Personally Identifiable Information Has Concrete Financial Value**

25. The private health information and personally identifiable information taken from MCG's system is particularly sensitive. Medical and personally identifiable information is valuable to cybercriminals and has routinely been sold and traded on the dark web.

26. PII and PHI are inherently valuable and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data breaches, 525 of them, or 35.64% were in the medical or healthcare industry. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

27. Identity theft results in a significant negative financial impact on victims as well as severe distress.

28. MCG is aware that the PII and PHI it collects is highly sensitive and of substantial value to those who would use it for wrongful purposes.

29. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud. There is a robust black market in which criminals openly post stolen PII and PHI on multiple underground internet websites, commonly referred to as the dark web.

30. There is accordingly a market for Plaintiffs' and Class members' PII and PHI.

31. Sensitive healthcare data can sell for as much as $363 per record, according to the Infosec Institute.

32. MCG states that medical codes were disclosed within the breach. Medical codes are used to convert diagnoses, procedures, medical services, and equipment into universal medical alphanumeric codes.

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.