UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

JULIE MACK, JOANNE MULLINS, and INGRID COX on behalf of themselves and all others similarly situated, Plaintiffs, vs. MCG Health, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Julie Mack, Joanne Mullins, and Ingrid Cox (collectively "Plaintiffs") individually and on behalf of all others similarly situated, through undersigned counsel, hereby allege the following against Defendant MCG Health, LLC ("MCG Health" or "Defendant"). The facts pertaining to Plaintiffs are alleged based upon personal knowledge, and all other facts herein are alleged based upon information and belief and the investigation of Plaintiffs' counsel.

NATURE OF THE ACTION

1. This is a class action for damages with respect to MCG Health, LLC for its failure to exercise reasonable care in securing and safeguarding patients' sensitive personal data—including names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender ("PII" or "Private Information").

2. This class action is brought on behalf of patients whose sensitive PII was stolen by cybercriminals in a cyber-attack on MCG Health's systems that took place in or around

March 25, 2020 and which resulted in the access and exfiltration of sensitive patient information (the "Data Breach").[1]

3. MCG Health reported to Plaintiffs and members of the putative "Class" (defined below) that information compromised in the Data Breach included their PII.

4. Plaintiffs and Class members were not notified of the data breach until, at the earliest, June of 2022—at least two years after their Private Information was first accessed.

5. As a result of the Data Breach and Defendant's failure to promptly notify Plaintiffs and Class members of the Data Breach, Plaintiffs and Class members have experienced and will experience various types of misuse of their PII in the coming months and years, including but not limited to, unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their Private Information.

6. There has been no assurance offered by MCG Health that all personal data or copies of data have been recovered or destroyed.

7. Accordingly, Plaintiffs assert claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, declaratory and injunctive relief, and state consumer protection claims.

PARTIES

A. Plaintiff Julie Mack

8. Plaintiff Julie Mack is a resident and citizen of Dallas, Texas and brings this action in her individual capacity and on behalf of all others similarly situated. Plaintiff Mack was an employee at Dallas Medical Center and has also received healthcare services through Dallas Medical Center in the past, including a visit to the hospital's emergency department in early 2020. To receive services at MCG Health, Plaintiff Mack was required to disclose her Private Information, which was then entered into MCG Health's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and

[1] *MCG Health, LLC Data Breach Notification Listing*, MT. DEP'T OF JUSTICE, https://dojmt.gov/consumer/databreach/ (follow "View Data Breaches Reported to Montana Office of Consumer Protection" hyperlink; then search for "MCG Health, LLC") (last visited July 5, 2022).

impliedly promised to safeguard Plaintiff Mack's Private Information. Defendant, however, did not take proper care of Plaintiff Mack's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

9. In June of 2022, Plaintiff Mack received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

10. Plaintiff Mack and Class members have faced and will continue to face a certainly impending and substantial risk of a slew of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

11. Some of these harms will not materialize for years after the Data Breach incident, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

12. Plaintiff Mack greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that her healthcare providers' data processor, MCG Health, would negligently maintain her Private Information as it did.

B. Plaintiff Joanne Mullins

13. Plaintiff Joanne Mullins is a resident and citizen of Bellville, Texas, and brings this action in her individual capacity and behalf of all others similarly situated. Plaintiff Mullins is a regular patient of Catholic Health Initiatives medical facilities including the Catholic Health Initiatives St. Joseph Health facility in Bellville, Texas for regular doctor and specialist visits. To receive services at MCG Health, Plaintiff Mullins was required to disclose her Private Information, which was then entered into MCG Health's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Mullins' Private Information. Defendant, however, did not take proper

care of Plaintiff Mullins' Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

14. In June of 2022, Plaintiff Mullins received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

15. Plaintiff Mullins and Class members have faced and will continue to face a certainly impending and substantial risk of a slew of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

16. These harms are not just theoretical. On September 23, 2021, an unauthorized actor used Plaintiff Mullins' PayPal account to charge $375 to her credit card for a denim jacket from a vendor called "Axel Arigato AB." Plaintiff Mullins did not make or authorize these charges. The product was scheduled to be shipped to an address in Bellflower, California. Plaintiff Mullins noticed the fraudulent charges on her account, and was able to file a "return to sender" request through UPS to send the item back to the seller before it was delivered to the fraudulently entered address that the hacker entered in her PayPal account. The credit card charge, however, remained on her account statement, resulting in Plaintiff Mullins spending approximately three hours reporting this fraudulent charge to PayPal customer service and filing an identity theft report with the Federal Trade Commission.

17. Given the fact that Plaintiff Mullins' Private Information was used to effectuate fraudulent charges on her credit card, she has suffered misuse of her information as a result of data breach on MCG Health's systems.

18. Fraudulent charges on a person's credit card are just one example of how cybercriminals can use individual's Private Information to perpetrate identity theft. Some of these harms will not materialize for years after the Data Breach incident, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

19. Plaintiff Mullins greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she known that her healthcare providers' data processor, MCG Health, would negligently maintain her Private Information as it did.

C. Plaintiff Ingrid Cox

20. Plaintiff Ingrid Cox is a citizen and resident of Slidell, Louisiana, and brings this action in her individual capacity and behalf of all others similarly situated. Plaintiff Cox is a regular patient of medical facilities around Slidell, Louisiana for regular doctor and specialist visits, but otherwise does not know how MCG Health would have obtained her information. To receive services at MCG Health, Plaintiff Cox was required to disclose her Private Information, which was then entered into MCG Health's database and maintained without her knowledge. In maintaining her Private Information, Defendant expressly and impliedly promised to safeguard Plaintiff Cox's Private Information. Defendant, however, did not take proper care of Plaintiff Cox's Private Information, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

21. In June of 2022, Plaintiff Cox received a notification letter from Defendant stating that her Private Information was compromised by cybercriminals.

22. Plaintiff Cox and Class members have faced and will continue to face a certainly impending and substantial risk of a slew of future harms as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

23. Some of these harms will not materialize for years after the Data Breach incident, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

24. Plaintiff Cox greatly values her privacy, especially while receiving medical services, and would not have paid the amount that she did to receive medical services had she

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.