John Heenan
Joseph P. Cook
HEENAN & COOK
1631 Zimmerman Trail
Billings, MT 59102
Phone: (406) 839-9091
Fax: (406) 839-9092
john@lawmontana.com
joe@lawmontana.com

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
GREAT FALLS DIVISION

ALLISON SMELTZ et al., on behalf of herself and all others similarly situated, Plaintiff, vs. LOGAN HEALTH and DOES I through X, Defendants.	Cause No. CV-22-28-GF-BMM-JTJ Judge **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Allison Smeltz (Plaintiff), individually and on behalf of the proposed class described herein, brings this action against Defendant Logan Health, and submits their Complaint and Demand for Jury Trial as follows:

INTRODUCTION

1. Plaintiff brings this action against Logan Health for its failure to protect her sensitive personal information, and the sensitive personal information of others similarly situated. Logan Health had access to such information through contracts it had with health care providers.

PARTIES

2. Plaintiff is a resident of Montana.

3. Logan Health is a domestic non-profit corporation.

4. Doe Defendants I through X are subsidiary, sister, or related entities of Logan Health who may be determined through discovery to bear responsibility for the actions described herein.

JURISDICTION & VENUE

5. The Court has diversity jurisdiction as the parties are residents of different states and the amount in controversy exceeds $75,000.

COMMON ALLEGATIONS

6. In February of 2022, Logan Health reported a data breach that compromised the personal identifying information ("PII") and protected health information ("PHI") of approximately 213,545 people including 174,761 Montanans. According to the notice, different information may have been compromised including name, address, medical record number, date of birth,

telephone number, email address, diagnosis and treatment codes, dates of service, treating/referring physician, medical bill account number and/or health insurance information, and Social Security numbers.

7. According to the notice, the breach occurred on November 18, 2021 and on November 22, 2021, Logan Health discovered suspicious activity including evidence of unauthorized access to a file server containing patient information. According to a Logan Health spokesperson, the perpetrator of the hack was a "malicious actor."

8. This data breach isn't the first time Logan Health has allowed patient information to be compromised. The hospital has also previously reported a January 2021 data breach to the Montana Attorney General's Office that affected 2,081 Montanans. In 2019, Logan Health, under its previous name of Kalispell Regional Healthcare, reported a breach to the Montana AG's Office that affected 126,805 Montanans. Following the 2019 breach, Logan Health claimed to be taking "further steps to revise procedures that will minimize the risk of a similar event happening again" and that "We...have taken steps to prevent similar events from occurring in the future."

9. The 2021 data breach occurred because, despite representations to the contrary, Logan Health failed to implement adequate and reasonable training of

employees and/or procedures and protocols which would have prevented the data breach from occurring.

10. Logan Health has identified Plaintiff as a victim of the data breach and has sent Plaintiff a letter informing her of such.

11. Logan Health was aware, or reasonably should have been aware, that a patient's sensitive personal information is of significant value to those who would use it for wrongful purposes.

12. A "cyber black market" exists in which criminals openly post stolen social security numbers and other personal information on multiple underground websites. Identity thieves can use sensitive personal information, such as that of Plaintiff and others similarly situated, to perpetrate a variety of crimes. According to the FBI Cyber Division, in an April 8, 2014 Private Industry Notification:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

13. Logan Health was aware, or reasonably should have been aware, that health care organizations such as it are a prime target of "malicious actors" hoping to gain access to PII and PHI.

14. The ramifications of Logan Health's failure to keep the affected patients' sensitive personal information secure are long lasting and severe. Once

sensitive personal information is stolen, fraudulent use of that information and damage to the affected patients may continue for years. As explained by the Federal Trade Commission:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making false claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[1]

Also, as reported by CreditCards.com:

> The Ponemon Institute found that 36 percent of medical ID theft victims pay to resolve the issue, and their out-of-pocket costs average nearly $19,000. Even if you don't end up paying out of pocket, such usage can wreak havoc on both medical and credit records, and clearing that up is a time-consuming headache. That's because medical records are scattered. Unlike personal financial information, which is consolidated and protected by credit bureaus, bits of your medical records end up in every doctor's office and hospital you check into, every pharmacy that fills a prescription and every facility that processes payments for those transactions.[2]

The average time spent by those respondents who successfully resolved their situation was more than 200 hours, working with their insurer or healthcare

---

[1] Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (accessed November 8, 2019).

[2] Cathleen McCarthy, CreditCards.com, *How to Spot and Prevent Medical Identity Theft*, available at www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php (accessed November 8, 2019).

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.