EXHIBIT A

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

ALAN HALL, individually and on behalf of all others similarly situated, Plaintiffs, v. SEA MAR COMMUNITY HEALTH CENTERS, Defendant.	Cause No. **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiff Alan Hall, individually, and on behalf of all others similarly situated, brings this action against Defendant Sea Mar Community Health Centers ("SMCHC" or "Defendant"), a Washington corporation," to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. SMCHC is a health-care provider that provides medical services to patients in the State of Washington.

2. Between the dates of December 2020 and March 2021, an unauthorized individual hacked SMCHC's IT network and obtained unauthorized access to confidential files containing current and former patients' Private Information (the "Data Breach").

3. For at least three months, the cybercriminals who hacked into SMCHC's IT network had unfettered access to files containing information pertaining to SMCHC patients (like Plaintiff).

4. Incredibly, the threat actor—known as the "Marketo gang"—stole 3 TB of sensitive data from SMCHC and thereafter posted it for sale on the "Marketo marketplace," a marketplace where the cybercriminals sell their stolen data to the highest bidder on the dark web.

5. Defendant only became aware of the hacking incident and Data Breach on June 24, 2021, when the unauthorized actor informed Defendant that it had successfully copied the sensitive data from its digital environment.

6. As a result of the Data Breach, Plaintiff and more than 650,000 Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of value of their personal information.

7. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

8. Information compromised in the Data Breach includes patient names, addresses, dates of birth, Social Security numbers, medical and clinical treatment information, insurance information, claims information and other protected health information as defined by the Health

Insurance Portability and Accountability Act of 1996 ("HIPAA") that Defendant collected and maintained (collectively the "Private Information").

9. SMCHC did not notify patients' that their Private Information was subject to unauthorized access in the Data Breach until October 2021, approximately ten (10) months after the cyberattack was launched and approximately four (4) months after the Data Breach discovered.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' and employees' Private Information.

11. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

12. Defendant SMCHC maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

13. Upon information and belief, the mechanism of the hacking and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

14. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and

reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

15. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for four (4) months.

16. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing

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.