IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA
MOBILE DIVISION

TAMMY PHILLPS, LOUIS LUMPKIN and ANTONIA FOXWORTH, *individually and on behalf of all others similarly situated,* Plaintiffs, v. COASTAL FAMILY HEALTH CENTER, Defendant.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs, TAMMY PHILLIPS, LOUIS LUMPKIN and ANTONIA FOXWORTH (the "Plaintiffs"), individually and on behalf of all others similarly situated, brings this action against Defendant COASTAL FAMILY HEALTH CENTER ("Coastal Family" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent ransomware attack and data breach that was perpetrated against Defendant Coastal Family, a not-for-profit community health center servicing southern Mississippi (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information (the "Private Information").

2. As a result of the Data Breach, Plaintiffs and approximately 62,342 Class Members[1] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The Private Information compromised in the Data Breach included names, addresses, Social Security numbers, health insurance information, and health and treatment information. The healthcare-specific data compromised is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and information such as Plaintiff's Social Security number is deemed personally identifiable information ("PII").

4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private

[1] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Sept. 15, 2021).

Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of a third party.

5. Upon information and belief, Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

6. Upon information and belief, the mechanism of the cyberattack 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 the risk of a ransomware attack.

7. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the PII and PHI that Coastal Family collected and maintained is now in the hands of data thieves.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, 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' health information to target

other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

9. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiffs and Class Members must now and in the future closely monitor their financial and medical accounts and information to guard against identity theft, among other issues.

10. Plaintiffs and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

11. Plaintiffs and Class Members have and may in the future expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

12. By their Complaint, Plaintiffs seek to remedy these harms on behalf of himself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, exemplary damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits and adequate credit monitoring services funded by Defendant.

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

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserts a claim for negligence.

PARTIES

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.