IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

HEATHER ERICA BETZ, on behalf of herself and all others similarly situated, Plaintiffs, v. ST. JOSEPH'S/CANDLER HEALTH SYSTEM, INC., Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Heather Erica Betz ("Plaintiff"), individually and on behalf of all others similar situated (collectively, the "Class," "Class Members," or "Plaintiffs"), by and through her attorneys, brings this Class Action Complaint against Defendant St. Joseph's/Candler Health System, Inc. ("Defendant" or "SJ/C"), seeking damages, restitution, and injunctive relief for the Class, upon investigation of her counsel, personal knowledge, facts that are a matter of public record, and information and belief as to all other matters.

NATURE OF THE ACTION

1. SJ/C is a healthcare provider rendering medical services to patients in 117 locations spanning 4,000 square miles of Georgia and South Carolina.

2. On or about December 18, 2020, unauthorized individuals hacked SJ/C's IT network and accessed the private and confidential medical information of approximately 1,400,000 individuals[1] (the "Data Breach"), including names, addresses, Social Security numbers, dates of birth, driver's license numbers, billing account information, financial information, health insurance information, employment information, family member and emergency contact information, medical record numbers, dates of service, provider names, and medical and clinical treatment information (collectively, "Personally Identifiable Information" or "PII" and "Personal Health Information" or "PHI").

3. For a full six months after these cyber criminals first accessed SJ/C's IT system, the hackers were able to move freely and undetected through the hospital system's IT network.[2]

4. It was not until June 17, 2021, that "SJ/C identified suspicious activity in its IT network."[3]

---

[1] Department of Health and Human Services Office of Civil Rights, *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Sept. 9, 2021).

[2] St. Joseph's/Candler, *Notice to Our Patients of a Data Security Incident*, https://www.sjchs.org/patient-privacy/policy/notice-to-our-patients-of-a-data-security-incident (last accessed Sept. 9, 2021).

[3] *Id.*

5. That "suspicious activity" detected on June 17, 2021 was the *coup de grâs* of the hackers' six-month attack. They were holding the hospital system's IT system hostage, and "demanding an as-yet unknown payment in order to release their hold on the system.[4]

> At approximately 4 a.m. on Thursday, June 17, all of the information systems at St. Joseph's/Candler Hospital system in Savannah went down. It wasn't a simple software glitch or temporary power outage. It was, instead, a complete information technology (IT) meltdown. Everything, from electronic medical record[s] (EMR) used to document encounters to the lab, radiology and billing software, went down. Even the phones, which are formatted as voice over internet protocol (VOIP) devices, stopped working. All of St. Joseph's/Candler usual patient encounter protocols were immediately rendered ineffective. The hospital system was, in essence, flying blind.[5]

6. Caught unaware, the hospital system was forced to improvise:

> [SJ/C went] "back to the future" with paper charting, handwritten notes, and lab runners taking lab and x-ray results to the floors, the emergency room and the operating room. For the system's 4,200 employees, 714-plus hospital beds between the two hospitals, and more than 500 doctors, the crisis forced and unexpected on-the-fly adaptation which increased the risk of error—and, potentially, of adverse patient outcomes.[6]

7. It took more than two weeks, until July 2, 2021, for the hospital's IT system to "slowly begin to come back online," but the reboot was "slow and

---

[4] Mark Murphy, *St. Joseph's/Candler Health System Cyberattack Offers Lessons for Us All*, Savannah Morning News (Jul. 9, 2021 at 6:00 AM), https://www.savannahnow.com/story/news/2021/07/09/learning-savannah-st-josephs-candler-hospitals-cyberattack/7907374002/.

[5] *Id.*

[6] *Id.*

deliberate," and it took much longer for the hospital to return to normal operations.[7]

8. On information and belief, SJ/C's rapid switch to pre-internet medical practice was necessitated by Defendant's failure to adequately and regularly back up data and/or failure to create a reasonable data recovery plan, despite having been warned to do so by multiple federal agencies, include the U.S. Department of Health and Human Services ("HHS"), the Cybersecurity and Infrastructure Security Agency ("CSIA"), and the Federal Bureau of Investigation ("FBI").[8]

9. SJ/C was on clear notice that cyber criminals were planning *precisely* this type of attack on hospitals.[9]

10. On June 4, 2020, HHS warned of the Maze Ransomware, which was being used to target healthcare organizations.[10] The HHS warning included detailed information on the Maze Ransomware, including file names that would be installed by hackers, where those file names could be found in a computer

---

[7] *Id.*

[8] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, AA20-302A (Oct. 28, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

[9] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware* (Nov. 18, 2019 at 9:44 PM), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware ("Senior FBI and U.S. Secret Service officials said Monday that cybercriminals are increasingly using ransomware to target vulnerable entities like hospitals and municipalities, and urged victims to report attacks to authorities regardless of whether they capitulate and pay ransoms.").

[10] HHS Cybersecurity Program, *Maze Ransomware*, Report # 202006041030 (Jun. 4, 2020), *available at* https://www.hhs.gov/sites/default/files/maze-ransomware.pdf.

system, IP addresses known to host the malware and launch it into hospitals' systems, the text and mechanisms of phishing emails used to gain access to the systems, web links known to launch the malware, commands associated with the malware, and several other tools for preventing and detecting precisely this type of attack.

11. On October 28, 2020, CSIA, FBI, and HHS issued an unprecedented joint advisory (the "Joint Cybersecurity Advisory") warning hospitals that they were in hackers' crosshairs.[11]

12. The Joint Cybersecurity Advisory again included detailed information on file names that would be installed by hackers, where those file names could be found in a computer system, IP addresses known to host the malware and launch it into hospitals' systems, the text and mechanisms of phishing emails used to gain access to the systems, web links known to launch the malware, commands associated with the malware, and several other tools for preventing and detecting precisely this type of attack.[12]

[11] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, AA20-302A (Oct. 28, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

[12] *Id.*; FireEye, *Threat Research Blog: Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser* (Oct. 28, 2020), https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html (blog linked in Joint Cybersecurity Advisory "[f]or a comprehensive list of indicators of compromise regarding the BazarLocker malware); FEDO Tracker, *Browse Botnet C&Cs* (last accessed Sept. 9, 2021), https://feodotracker.abuse.ch/browse/trickbot/ (linked to in Joint Cybersecurity Advisory as "an open source tracker for Trickbot C2 servers).

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.