UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

TENNIE KOMAR, on behalf of herself and all others similarly situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Tennie Komar ("Plaintiff") brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendant**,** Shields Health Care Group, Inc. ("Shields" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE CASE

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time

and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a healthcare provider, Shields knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

4. Shields's Privacy Practice informs patients "how medical information about [patients] may be used and disclosed how [they] can get access to [that] information."[1] The Privacy Practice acknowledges Shields's duty to maintain the privacy of patients' health information.

5. Plaintiff brings this class action on behalf of individual patients who used Shields's services whose PII and/or PHI were accessed and exposed to unauthorized third parties during a data breach of Shields's system, which Shields states occurred between March 7, 2022, and March 28, 2022 (the "Data Breach") and involved the "managing and imaging services" Shields provides for approximately 56 distinct "facility partners."

6. Despite that Shields became aware of the Data Breach by March 28, 2022,[2] it failed to notify Plaintiff and the putative Class members within 60 days as required by law. Notably, Shields failed to notify Plaintiff of the Data Breach for more than two months from its discovery of the same.

7. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

---

[1] Shields Health Care Group, *Privacy*, https://shields.com/privacy/ (last accessed June 27, 2022).
[2] Shields Health Care Group, *Notice of Data Security Incident*, https://shields.com/notice-of-data-security-incident/ (last accessed June 27, 2022).

8. Based on the public statements of Shields to date, a wide variety of PII and PHI was implicated in the breach, including full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medial or treatment information.[3]

9. As a direct and proximate result of Shields's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff and Class Members' PII and PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

10. Plaintiff and Class Members are now at a significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

11. To recover from Shields for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Shields to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Shields; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

12. Plaintiff Tennie Komar is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Massachusetts and was a patient of Defendant's, receiving services at the following facilities:

[3] *Id.*

a. Emerson Hospital located at 133 Old Road to Nine Acre Corner, Concord, Massachusetts 01742; and

b. UMass Memorial Hospital HealthAlliance Hospital Leominster located at 100 Hospital Road, Suite 1A, Leominster, Massachusetts 01453.

13. Defendant Shields is a Massachusetts corporation with its principal place of business in this District, and a substantial part of the events raising out of the claims alleged occurred within this District.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

15. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business is in Massachusetts.

16. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(1), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District. Further, Defendant has its principal place of business in this District.

FACTUAL BACKGROUND

A. Shields Health Care Group and the Services Provided

17. Shields is a for-profit company that provides management and imaging services on behalf of several dozen partner facilities in the New England region, including Massachusetts, Maine, and New Hampshire.[4]

[4] Shields Health Care Group, *Find a Location*, https://shields.com/find-location/ (last accessed June 27, 2022).

18. Shields provides services such as MRI, PET/CT, ASC, Radiation Oncology, and Ambulatory Surgical Centers.[5]

19. The company provides services to many thousands of patients a year.

20. While administering these services and treatment, Defendant on a daily basis receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' full name, address, date of birth, Social Security number, other contact information, diagnosis, billing information, insurance information, medical records, patient ID, and other necessary information for treatment at the facilities.

21. Patients must entrust PII and PHI to Defendant to receive care, and in return, they reasonably expect that Defendant will safeguard their highly sensitive information and keep their PHI confidential.

22. Defendant refers to patients' information as "protected health information" and promises disclosure of highly sensitive personal information will only occur for the "purpose of treatment, payment or health care operations." [6]

B. Shields Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

23. At all relevant times, Shields knew it was storing sensitive PII and PHI and that, as a result Shields's systems would be attractive for cybercriminals.

24. Shields also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

25. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

---

[5] Shields Health Care Group, *Our Services*, https://shields.com/our-services/overview/ (last accessed June 27, 2022).
[6] Shields Health Care Group, *supra* note 1.

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.