UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

WILLIAM BISCAN, individually and on behalf of all others similarly situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP INC., Defendant.	**CIVIL ACTION NO.: _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff William Biscan, ("Plaintiff") individually and on behalf of all others similarly situated, bring this action against Defendant Shields Health Care Group Inc. ("Shields" or "Defendant"), a Massachusetts corporation, to obtain damages, restitution, and injunctive relief for himself and 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. This class action arises out of a targeted cyber-attack at Defendant's medical facilities that allowed a third party to access Defendant's computer systems and data from approximately March 7, 2022 to March 21, 2022, exposing highly sensitive personal information and medical records of approximately two million patients from Defendant's computer network (the "Data Breach").

2. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a diminution in the value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the

Data Breach.

3. Plaintiff's and Class Members' sensitive and private personal information—which was entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen as a result of the Data Breach. Information compromised in the Data Breach includes names, addresses, dates of birth, Social Security numbers, insurance information, medical record numbers, patient identification numbers, and other protected health information as defined by the HIPAA, and other personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively, "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, for failing to provide timely and adequate notice to Plaintiff and other Class Members of the unauthorized access to their Private Information by an unknown third party, and for failing to provide timely and adequate notice of precisely what information was accessed and stolen.

5. Defendant owed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

6. Defendant breached its duty to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and/or reckless manner.

7. Upon information and belief, the means of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable risks to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a

dangerous and vulnerable condition.

8. Defendant and its employees failed to properly monitor the computer network and systems housing the Private Information.

9. Had Defendant properly monitored its property, it would have discovered the intrusion sooner or been able to wholly prevent it.

10. Exacerbating an already devastating privacy intrusion, 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.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including 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, 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.

12. As a direct result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened 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.

13. Plaintiff and Class Members have, and will continue, to incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Data Breach and subsequent exposure of

their Private Information, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam messages and e-mails received as a result of the Data Breach. Plaintiff and Class Members have suffered and will continue to suffer an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their PII and PHI. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII and PHI as thieves will continue to use the information to obtain money and credit in their names for several years.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or removed from Defendant's network during the Data Breach.

16. Plaintiff seeks 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/identity protection services funded by Defendant.

17. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct asserting claims for negligence, breach of contract, breach of implied contract, invasion of privacy, breach of fiduciary duty, breach of confidence, violation of the Massachusetts Regulation of Business Practices for Consumers' Protection Act, Mass. Gen. Laws Ann. ch. 93A, § 1 *et seq*., and unjust enrichment.

PARTIES

18. Plaintiff Biscan is, and at all times mentioned herein was, an individual citizen of

Haverhill, Massachusetts. Plaintiff Biscan was a patient of Shields through its services at Winchester Hospital / Shields MRI, LLC.

19. Defendant Shields Health Care Group Inc. is a domestic corporation organized and existing under the laws of the Commonwealth of Massachusetts with its headquarters in Quincy, Massachusetts.

JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendant because Defendant is a resident of the Commonwealth of Massachusetts and because Defendant conducts business transactions in Massachusetts, has committed tortious acts in Massachusetts, and sells its products and services in Massachusetts. The Court has personal jurisdiction over Plaintiff because he resides in the Commonwealth of Massachusetts.

21. Jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d), as minimal diversity exists, there are more than 100 class members, and the amount in controversy is in excess of $5 million.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant is "the largest network of MRI centers in New England,"[1] with "more than 40 healthcare facilities throughout New England" including locations in Massachusetts, Maine, and New Hampshire.[2]

23. Defendant's business includes providing MRI, PET/CT, Radiation Oncology, and

[1] Shields Health Care Group, *Our Services*, available at https://shields.com/our-services/overview/ (last accessed June 9, 2022).
[2] Shields Health Care Group, *Find a Location*, available at https://shields.com/find-location/ (last accessed June 9, 2022)

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.