UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ROBERT HARTIGAN, on behalf of himself and all others similarly situated, Plaintiff, v. MACY'S, INC., Defendant.	)	Civil Action No. 20-10551-PBS

MEMORANDUM AND ORDER

November 5, 2020

Saris, D.J.

INTRODUCTION

This case is about a criminal cyberattack on the online database of defendant Macy's, Inc. ("Macy's"), a well-known department store chain -- its second hacking in less than a year and a half. Plaintiff Robert Hartigan ("Hartigan") brings this putative class action against Macy's alleging unreasonable interference with privacy in violation of M.G.L. c. 214, § 1B (Count I), negligence (Count II), breach of contract (Count III), unfair and deceptive business practices in violation of M.G.L. c. 93A, §2 (Count IV), and violation of M.G.L. c. 93H (Count V). Macy's moves to dismiss the action for lack of standing pursuant

to Fed. R. Civ. P. 12(b)(1) and for failure to state a claim pursuant to Fed. R. Civ. P. 12(b)(6).

After hearing, the Court **ALLOWS** Macy's motion to dismiss primarily on the ground of lack of standing.

FACTUAL BACKGROUND

Except where stated, the following facts are alleged in the First Amended Class Action Complaint and must be taken as true at this stage. See Newman v. Lehman Bros. Holdings Inc., 901 F.3d 19, 25 (1st Cir. 2018). The Court may also consider additional evidence in determining a motion to dismiss pursuant to Fed. P. Civ. P. 12(b)(1). Merlonghi v. United States, 620 F.3d 50, 54 (1st Cir. 2010) (citation omitted).

On October 10, 2019, Hartigan, a resident of Massachusetts, purchased items through Macy's website with his VISA credit card. He provided his home address, credit card information, and other personal information to complete the purchase.

Between October 7 and 15, 2019, hackers installed malware on Macy's website in order to access payment information of customers who completed online purchases. The personal information obtained included: (1) first and last names; (2) addresses; (3) phone numbers; (4) email addresses; and (5) credit card numbers, including expiration dates and security codes. A similar breach of Macy's data had occurred in May and June 2018. See Memorandum

Opinion at 2, Carroll v. Macy's Inc., No. 18-01060 (N.D. Ala. June 5, 2020).

Macy's privacy policy states it "put in place various procedural, technical, and administrative measures to safeguard the information [Macy's] collect[s] and use[s]." Dkt. 19 at 38-39. The policy also warned users that "no security safeguards or standards are guaranteed to provide 100% security." Id. at 39.

On November 14, 2019, Macy's sent a Breach Notification Letter to Hartigan and other Macy's customers about the data infringement. The breach notice provided information regarding the known risks of harm associated with data breaches, as well as steps that customers could take to protect themselves from data infringement. To address the heightened risk of personal identity theft, Macy's offered Hartigan one year of complimentary credit monitoring services.

As a result of the hack, Hartigan alleges he suffered emotional distress, a breach of privacy, public disclosure of private facts, and loss of time. To mitigate against the risk of identity theft, Hartigan purchased data monitoring services from LifeLock.

DISCUSSION

The primary issue is whether Hartigan has pled sufficient injury-in-fact to establish standing. Macy's argues that Hartigan

has failed to do so because he has not alleged that he suffered economic harm, that his immutable personal information like a social security number has been misused, or that he faces imminent risk of future identity theft. Hartigan disagrees, contending that he has pled sufficient injury-in-fact based on his allegations that he suffers from increased risk of identity theft, that he has incurred costs to purchase credit monitoring services, and that he lost the benefit of the bargain because Macy's breached its contract with him.

I. Standing

"The party invoking the jurisdiction of a federal court carries the burden of proving its existence." Murphy v. United States, 45 F.3d 520, 522 (1st Cir. 1995) (citation omitted). In analyzing whether a complaint states a basis for jurisdiction under Rule 12(b)(1), the Court "must credit the plaintiff's well-[pleaded] factual allegations and draw all reasonable inferences in the plaintiff's favor." Merlonghi, 620 F.3d at 54. Standing is a jurisdictional issue properly challenged under Rule 12(b)(1). See United States v. AVX Corp., 962 F.2d 108, 113 (1st Cir. 1992).

To satisfy Article III standing, a plaintiff bears the burden of establishing three elements: (1) that he has suffered an "injury-in-fact" that is "concrete and particularized" and "actual

or imminent"; (2) that the injury is "'fairly traceable' to the actions of the defendant"; and (3) that the injury will likely be redressed by a favorable decision. Bennett v. Spear, 520 U.S. 154, 167 (1997) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992)). Each element must be proved "with the manner and degree of evidence required at the successive stages of the litigation." Id. at 167-68. The Supreme Court has held that a plaintiff threatened with future injury has standing to sue if the threatened injury is "certainly impending" or there is a "substantial risk that the harm will occur." See Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414, n. 5 (2013) (citation omitted).

II. Risk of Future Harm

The First Circuit has developed a helpful framework for considering whether an increased risk of future harm can constitute sufficient injury-in-fact to satisfy the standing requirement. See Kerin v. Titeflex Corp., 770 F.3d 978, 979-81 (1st Cir. 2014) (product liability ligation involving the risk of a product being vulnerable to failure after a lightning strike). It held that cases alleging increased risk of future harm, "potentially involve two injuries: (1) a possible future injury that may or may not happen (i.e. the harm threatened); and (2) a present injury that is the cost or inconvenience created by the increased risk of the first, future injury (e.g., the cost of mitigation)." Id. at 981-982 (citation omitted). Urging Courts to act "cautiously," it added

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.