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

that even if "one of the alleged injuries is present, satisfying imminence, the injury may still be speculative." Id. at 982.

Pre-Clapper, two First Circuit cases directly addressed whether risk of identity theft constitutes injury-in-fact. In the first case, Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011), involving a theft of electronic data by sophisticated thieves, the First Circuit found injury-in-fact where more than 1,800 fraudulent uses of customers' stolen credit card information had already occurred, and it reasonably appeared that all customers who used credit or debit cards during the class period "were at risk of unauthorized charges." Id. at 164. The following year in an action against a brokerage firm which failed to protect sensitive nonpublic personal information, the First Circuit held that the plaintiff had not demonstrated injury-in-fact because there was no allegation that the plaintiff's "nonpublic personal information has actually been accessed by an unauthorized user." Katz v. Pershing, LLC, 672 F.3d 64, 79 (1st Cir. 2012). The First Circuit further held that the plaintiff's purchase of identity theft insurance and credit monitoring service to guard against the "possibility, remote at best, that her nonpublic personal information might someday be pilfered" was insufficient because "a purely theoretical possibility simply does not rise to the level of a reasonably impending threat." Id. at 79-80.

Circuit courts have taken different paths in analyzing the risk of future harm in data breach cases. Recently, the D.C. Circuit found a "substantial risk" of identity theft is plausibly alleged when hacked data included sensitive personal information such as social security numbers, birthdates, and credit card numbers, even when there was no subsequent criminal activity. See Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017) (finding a substantial risk of harm existed "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); see also Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing where a stolen laptop contained employees' unencrypted social security numbers and other personal information).

Other courts have found injury-in-fact when the theft of personal data was followed by criminal activity. See Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015) (plaintiff alleged 9,200 fraudulent uses of stolen credit card information); Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (plaintiffs alleged fraudulent use of stolen social security numbers to open new credit cards and apply for credit); cf. In re Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018) (finding standing where hackers stole sensitive personal information and some hacked customers in parallel litigation suffered financial harm); Lewert v. P.F. Chang's China

Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (finding standing where plaintiff had fraudulent credit card charges made against his account even though no financial harm was suffered because the fraudulent charges were stopped by his bank).

Three circuits have declined to find standing where there were no allegations of criminal activity involving the stolen information, even when the data involved deeply personal information like social security numbers. See In re SuperValu, Inc., 870 F.3d 763, 768-70 (8th Cir. 2017) (holding no injury-in-fact where stolen information included names, payment card numbers, expiration dates, card verification codes, and personal identification numbers); Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (holding that even where social security numbers and other personal information were hacked, "the mere theft of these items, without more, cannot confer Article III standing"); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44, (3d Cir. 2011) (holding that even where names, social security numbers, birth dates, and bank accounts may have been exposed to a hacker, there was no injury-in-fact because "no identifiable taking occurred; all that is known is that a firewall was penetrated").

Here, even under the caselaw most generous to finding standing, Hartigan has not alleged sufficient facts to support a substantial risk of future harm for three reasons. First, there

are no allegations of any fraudulent use or even attempted use of the personal information to commit identify theft with respect to any Macy's customer whose credit information was stolen. Second, the information stolen was not highly sensitive or immutable like social security numbers. Third, immediate cancellation of a credit card can effectively eliminate risk of credit card fraud in the future. To be sure, even if the credit card is canceled, there is still some risk of future harm involving identify theft (like use of the customer's name, email, and home address), but it is not substantial and, at best, speculative.

III. Actual Harm by Cost of Mitigation

Alternatively, Hartigan has alleged actual harm because of the cost of mitigation. In his view, one year of credit monitoring is not satisfactory to protect against the risk of personal identity theft, and so he purchased a product called LifeLock to get better protection. The First Circuit has held that incurring credit monitoring costs as a mitigation measure can constitute injury-in-fact where plaintiffs' credit card information has been misused after a data breach. Anderson, 659 F.3d at 165. However, "[w]here neither the plaintiff nor those similarly situated have experienced fraudulent charges resulting from a theft or loss of data, the purchase of credit monitoring services may be unreasonable and not recoverable." Id. at 165 n. 10; see also Katz,

672 F.3d at 79 (holding that cost of identity theft insurance and credit monitoring services did not constitute injury-in-fact where there was no evidence of a data breach because "a possibility, remote at best, that [plaintiffs'] nonpublic personal information might someday be pilfered . . . simply does not rise to the level of a reasonably impending threat"); Clapper, 568 U.S. at 416 (holding that a plaintiff "cannot manufacture standing merely by inflicting harm on [himself] based on [his] fears of hypothetical future harm that is not certainly impending"). Other circuits have taken a similar approach. See Beck, 848 F.3d at 276 (holding no injury-in-fact based on monitoring costs "incurred in response to a speculative threat . . . of future identity theft") (citation omitted); In re SuperValu, Inc., 870 F.3d at 771 ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." (citing Clapper, 568 U.S. at 415)).

Here, although a data breach occurred, Hartigan alleges no misuse of his or any class member's data. Hartigan's purchase of credit monitoring services thus was not "premised on a reasonably impending threat" and does not constitute injury-in-fact. See Katz, 672 F.3d at 79. While it is certainly a hassle and annoying to cancel a credit card and contact all accounts using that card

for billing, there is no allegation of economic loss which flowed from this inconvenience.

IV. Loss of the Benefit of the Bargain

Finally, Hartigan argues that he suffered "loss of the benefit of the bargain" as a result of Macy's breach of contract. Specifically, he says he did not receive what he paid $191.75 for. The breach of a contractual right can constitute an injury sufficient to create standing. Katz, 672 F.3d at 72. Hartigan alleges that Macy's did not comply with its own rules or company policy to protect its customers' personal information.

Macy's policy states that Macy's "put in place various procedural, technical, and administrative measures to safeguard the information [Macy's] collect[s] and use[s]," and cautioned that "no security safeguards or standards are guaranteed to provide 100% security." Dkt. 19 at 38–39. The Court assumes, without deciding, that the breach of a privacy policy at a company can constitute a breach of contract in certain circumstances. See e.g., Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016) (finding injury-in-fact based on breach of contract where plaintiff alleged that defendant deliberately shared plaintiff's information with Facebook, in violation of the privacy policy in its contract).

Even if Hartigan thus has standing under a "loss of the benefit of the bargain" theory, however, this argument cannot survive Macy's motion to dismiss for failure to state a claim. See Fed. R. Civ. P. 12(b)(6). Hartigan fails to allege specific facts that plausibly support his claim that Macy's breached its privacy policy. See Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) ("To survive a [12(b)(6)] motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). Because Hartigan's conclusory assertion that Macy's did not comply with its privacy policy cannot meet Twombly's plausibility standard, the Court grants Macy's motion to dismiss this claim on 12(b)(6) grounds. See Twombly, 550 U.S. at 570.

ORDER

For the reasons stated above, Macy's motion to dismiss (Dkt. 20) is **ALLOWED** with prejudice.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge