IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

SPRINGMEYER ET AL.	*	
V.	*	**Case No. 20-cv-867-PWG**
MARRIOTT INTERNATIONAL, INC.	*	

* * * * * * * * * * * * * *

MEMORANDUM OPINION

This case involves the class action complaint filed by Pati Springmeyer and Joe Lopez on behalf of themselves and all others similarly situated following a data breach of Defendant Marriott that occurred in early 2020. Plaintiffs allege that their personal information, along with that of approximately 5.2 million other guests, was improperly accessed. Plaintiffs bring eleven claims under various common law and statutory causes of action. Marriott moves to dismiss, arguing that Plaintiffs lack standing and failed to state a claim.[1] For the reasons discussed below, Plaintiffs' claims are dismissed for lack of standing because they fail to adequately plead that their alleged injuries are fairly traceable to Marriott's conduct.

Factual Background

Marriott is a global hotel and hospitality chain with more than 7,000 properties in 130 countries, headquartered in Bethesda, Maryland. ECF No. 36, First Amended Class Action Complaint ("Compl.") ¶ 25. On March 31, 2020, Marriott announced a data breach affecting approximately 5.2 million guests. *Id.* ¶ 23–24. On that day, Marriott sent an email to affected guests and posted an incident notification on its website. *Id.* ¶ 24. The incident notification stated

[1] The motion has been fully briefed. *See* ECF Nos. 40, 41, 42, and 43. A hearing is not necessary. *See* Loc. R. 105.6 (D. Md. 2018).

that at the end of February 2020, Marriott identified that "an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property." *Id.* The notice said that Marriott believed the activity started in mid-January 2020. *Id.* After Marriott discovered the unauthorized access, it stated that it disabled the login credentials, began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests. *Id.*

Marriott stated that it believed that the guest information that was accessed may have including the following, but that all this information was not present for every guest:

- Contact Details (e.g., name, mailing address, email address, and phone number)
- Loyalty Account Information (e.g., account number and points balance, but not passwords)
- Additional Personal Details (e.g., company, gender, and birthday day and month)
- Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers)
- Preferences (e.g., stay/room preferences and language preference)

Id. Marriott stated that its investigation was ongoing but had no reason to believe that the information involved included loyalty account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers. *Id.*

Plaintiffs Springmeyer and Lopez both allege that they stayed at Marriott properties, gave Marriott their personal identifying information ("PII"), and received the notice that their PII had been accessed without authorization. *Id.* ¶¶ 11, 17. Plaintiffs allege that since the data breach, they have each spent time monitoring their accounts to protect the integrity if their PII and to detect and prevent any misuse of their PII. *Id.* ¶¶ 13–14, 18–19. Marriott has offered Plaintiffs one year of free enrollment in Experian's IdentityWorks credit monitoring service. *Id.* ¶ 71. Nonetheless, Plaintiff Springmeyer alleges that she purchased credit monitoring services at an annual cost of

$159.96. *Id.* ¶ 12. Plaintiffs allege that this data breach and their alleged damages were the result of Marriott's failure to implement appropriate safeguards for its guests' PII. *Id.* ¶ 65.

Pending is Defendant's motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Defendant argues that Plaintiffs lack standing and failed to state a claim upon which relief could be granted.

Discussion

I. Standing

Marriott argues that Plaintiffs do not have standing, and therefore this Court lacks subject matter jurisdiction over their claims.

a. Standard of Review

Marriott moves to dismiss for lack of standing under Federal Rule of Civil Procedure 12(b)(1). Under Rule 12(b)(1), the plaintiff bears the burden of proving, by a preponderance of evidence, the existence of subject matter jurisdiction. *See Demetres v. E. W. Constr., Inc.*, 776 F.3d 271, 272 (4th Cir. 2015); *see also Evans v. B.F. Perkins Co.*, 166 F.3d 642, 647 (4th Cir. 1999). A challenge to subject matter jurisdiction under Rule 12(b)(1) may proceed in two ways: either by a facial challenge, asserting that the allegations pleaded in the complaint are insufficient to establish subject matter jurisdiction, or a factual challenge, asserting "'that the jurisdictional allegations of the complaint [are] not true.'" *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009) (citing *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)) (alteration in original); *see Buchanan v. Consol. Stores Corp.*, 125 F. Supp. 2d 730, 736 (D. Md. 2001). Here Marriott brings a facial challenge to Plaintiffs' Article III standing. In a facial challenge, "the facts alleged in the complaint are taken as true, and the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns*, 585 F.3d at 192. However, "[a]

pleading that offers labels and conclusions or a formulaic recitation of the elements of a cause of action" or "naked assertions devoid of further factual enhancement" will not suffice. *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 623 (4th Cir. 2018) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

b. Application

To establish standing, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). The Court focuses its discussion on the second element.

To meet the "fairly traceable" requirement, Plaintiffs must allege facts to plausibly show that their alleged injuries were the result of Defendant's conduct. This standard "is not equivalent to a requirement of tort causation." *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d at 623 (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 161 (4th Cir. 2000)). "When a complaint is evaluated at the pleading stage . . . 'general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.'" *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561(1992)). But the "[p]leadings must be something more than an ingenious academic exercise in the conceivable." *Id.* (quoting *United States v. Students Challenging Regulatory Agency Procedures (SCRAP)*, 412 U.S. 669, 688 (1973)). "Where, as here, a case is at the pleading stage, the plaintiff must 'clearly . . . allege facts demonstrating' each element" of standing, including traceability. *Spokeo, Inc. v. Robins*, 136 S. Ct. at 1547 (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)). As in this case, when the actions of a third party are involved, "[t]he 'case or controversy' limitation of Art. III

still requires that a federal court act only to redress injury that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court." *Doe v. Obama*, 631 F.3d 157, 161 (4th Cir. 2011) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)).

Here Plaintiffs must allege facts for the Court to plausibly infer that the unauthorized access of Plaintiffs' PII by an unspecified bad actor or actors using Marriott employee credentials is fairly traceable to Marriott's conduct.[2] In this regard Plaintiff attempts to plead the fairly traceable element by alleging that the data breach and their injuries are a result of "Marriott's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its guests' PII." *Id.* ¶ 5. But "the[se] allegations are conclusory and not entitled to be assumed true." *Ashcroft v. Iqbal*, 556 U.S. at 681. Plaintiffs fail to allege any facts describing Marriott's cybersecurity or steps that it could have or should have taken to prevent this data breach. To be sure, Plaintiffs repeat their conclusory allegations that Marriott's cybersecurity was unreasonable throughout the Complaint in connection with their eleven causes of action. For example, Plaintiffs allege the following:

> Marriott disregarded the rights of Plaintiffs and Class Members . . . by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data and cyber security systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard guest PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and accurate notice of the Data Breach.

[2] Plaintiffs do not specify whether it was Marriott employees that used their credentials to access Plaintiffs' PII without authorization or whether a third party gained access to the Marriott employees' credentials to do so. In either case, Plaintiffs do not allege that Marriott was responsible for the attack by virtue of its status as an employer.

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.