**UNITED STATES DISTRICT COURT**

**DISTRICT OF CONNECTICUT**

| | | |
|---|---|---|
| YANKOVICH, et al,<br>*Plaintiffs*, | ) | 3:21-CV-00720 (KAD) |
| v. | ) | |
| APPLUS TECHNOLOGIES, INC.,<br>*Defendant*. | ) | |
| | ) | AUGUST 9, 2022 |

**MEMORANDUM OF DECISION RE: DEFENDANT'S MOTION TO DISMISS (ECF NO. 12)**

Kari A. Dooley, United States District Judge

This class action arises out of a malware attack against Defendant, Applus Technologies, Inc., which allegedly resulted in the compromise of personal identifying information ("PII") belonging to Plaintiffs, Amelia Yankovich and Joseph Allen, and those similarly situated. In a two-count Complaint, Plaintiffs assert state law claims for negligence and breach of implied contract, alleging that the malware attack provided cybercriminals with access to their confidential, sensitive, "non-public" PII which could be used to perpetrate identity theft or other fraud. Pending before the Court is Defendant's motion dismiss both counts of the Complaint pursuant to Fed. R. Civ. P. 12(b)(1) for lack of Article III standing. Defendant argues that all of Plaintiffs' PII compromised in the malware attack was publicly available information, and as such Plaintiffs have not sufficiently established an injury in fact for purposes of demonstrating Article III standing. For the reasons set forth below, the motion to dismiss is GRANTED.[1] (ECF No. 12)

**Standard of review**

[1] Defendant has also moved to dismiss Plaintiffs' Complaint pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a plausible claim for relief. Because the Court concludes that Plaintiffs lack Article III standing, it need not and does not address Defendant's alternative arguments pursuant to Rule 12(b)(6).

Article III, Section 2 of the Constitution limits the subject-matter jurisdiction of the federal courts to "Cases" and "Controversies." *SM Kids, LLC v. Google LLC*, 963 F.3d 206, 211 (2d Cir. 2020). The standing doctrine, which emerges from Article III, is designed "to ensure that federal courts do not exceed their authority as it has been traditionally understood." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). A plaintiff has Article III standing when the plaintiff has "(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 judicial decision." *Id*. In a class action, federal courts lack jurisdiction if no named plaintiff has standing. *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019). The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements, "which must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e*., with the manner and degree of evidence required at successive stages of litigation." *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300 (2d Cir. 2021) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that it exists. *Katz v. Donna Karan Co., L.L.C*., 872 F.3d 114, 119 (2d Cir. 2017).[2]

A motion to dismiss for lack of Article III standing is properly brought under Fed. R. Civ. P. 12(b)(1). *SM Kids*, 963 F.3d at 210. When a motion under Rule 12(b)(1) is based solely on the complaint and the attached exhibits, the plaintiff bears no evidentiary burden. *Id*. In addressing such a "facial" challenge, the task of the district court is to determine whether, after accepting as true all material factual allegations of the complaint and drawing all reasonable inferences in favor

[2] Additionally, "[w]here . . . jurisdiction is predicated on diversity of citizenship, a plaintiff must have standing under both Article III of the Constitution and applicable state law in order to maintain a cause of action." *Mid-Hudson Catskill Rural Migrant Ministry, Inc. v. Fine Host Corp.*, 418 F.3d 168, 173 (2d Cir. 2005). "This requirement that a plaintiff have standing under both Article III and state law ensures that a federal court sitting in diversity does not exceed its limited jurisdiction." *Rondina v. Feigenbaum*, No. 3:19-CV-01699 (KAD), 2021 WL 243082, at *3 (D. Conn. Jan. 25, 2021) (citing *City of Indianapolis v. Chase Nat. Bank of City of New York*, 314 U.S. 63, 76 (1941)). Defendant does not challenge Plaintiff's standing under Connecticut law.

of the plaintiff, the alleged facts affirmatively and plausibly suggest that the court has subject matter jurisdiction. *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56–57 (2d Cir. 2016). A motion under Rule 12(b)(1) may also rely on evidence beyond the pleadings. *SM Kids*, 963 F.3d at 210. When a defendant makes such a fact-based motion, the plaintiff may respond with evidence of its own. *Id*. However, "plaintiffs *must* come forward with evidence of their own to controvert that presented by the defendant," unless "the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing," in which case, the plaintiff may rely on those allegations. *Katz*, 872 F.3d at 119 (internal quotation marks omitted) (emphasis added). In other words, if the affidavits submitted on a 12(b)(1) motion "reveal the existence of factual problems" in the assertion of jurisdiction, the plaintiffs "will need to come forward with evidence of their own to controvert that presented by the defendant." *Carter*, 822 F.3d at 57.

**Factual Allegations**

Plaintiff's Complaint is summarized as follows. Defendant is a Delaware corporation that manages vehicle inspections and emission testing and services for Connecticut drivers on behalf of the Connecticut Department of Motor Vehicles ("CT DMV"). Plaintiff class members consist of Connecticut motorists who have registered their vehicles with the CT DMV. Plaintiffs' PII was provided to Defendant as a condition of Plaintiffs registering their vehicles with the CT DMV and utilizing vehicle emissions testing managed by Defendant.[3]

On or about March 30, 2021, Defendant learned that it was the victim of a malware attack perpetrated by cybercriminals, which resulted in a data breach that provided these cybercriminals

[3] Defendant's Software Development Manager, Bradley, S. Zygmunt, stated in an August 11, 2021 affidavit that Defendant does not itself perform emissions testing, but rather contracts with service stations which license Defendant's emissions testing technology.

with access to Plaintiffs' PII. Following the data breach, Defendant temporarily shut down its vehicle emissions testing programs in eight states, including Connecticut. Defendant retained computer forensic experts to determine the nature of the malware attack and extent of PII that had been compromised. Defendant further advised customers to "monitor your financial accounts for any unauthorized activity and alert authorities and your bank if you see anything unusual."

Plaintiffs do not know with certainty the specific type of malware used during the attack or the extent to which Connecticut vehicle owners' PII was impacted.[4] Plaintiffs rely upon news reports that suggest that Defendant "was likely targeted by a ransomware attack" and the extent of compromised PII "could include information about vehicles and their owners." Plaintiffs allege that the PII that was likely compromised in the malware attack was confidential, sensitive, "non-public" information. Specifically, Plaintiffs allege that the PII provided to Defendant and compromised in the malware attack included their names, addresses, dates of birth, personal identification numbers, Social Security numbers, driver's license numbers, and license plate numbers.

Plaintiffs do not allege that they, or anyone, have experienced identity theft or fraud as a result of the data breach. Rather, Plaintiffs allege that, as a direct result of Defendant's failure to maintain the security and confidentiality of their PII and because their PII is now readily available on the internet, they and others similarly situated "now and for the rest of their lives face an imminent, heightened, and substantial risk of identity theft and other fraud." It is this heightened risk of injury which Plaintiffs rely upon to establish an injury in fact.

[4] Plaintiffs allege that Defendant "has not yet disclosed the specific type of malware used during the attack" or "the extent to which Connecticut vehicle owners' PII was impacted." Plaintiffs further contend that Defendant "refuse[d] to disclose pertinent details" regarding the data breach and its subsequent investigation. Defendant disputes this allegation. In an October 7, 2021 affidavit, Defendant's counsel, Attorney John A. Vogt, avers that, although Defendant "did not provided Plaintiffs with a forensic report relating to the incident," Defendant informed Plaintiffs' counsel before filing its motion to dismiss that "the investigation did not identify evidence that the server that housed the data regarding Connecticut residents was accessed" in the malware attack.

**Discussion**

"The Supreme Court has made clear that 'allegations of possible future injury' or even an 'objectively reasonable likelihood' of future injury is insufficient to confer standing." *McMorris,* 995 F.3d at 300 (quoting *Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409–10 (2013)). "Rather, a future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" *Id.* (quoting *Susan B. Anthony List v. Driehaus,* 573 U.S. 149, 158 (2014)). In *McMorris,* the Second Circuit Court of Appeals joined its sister Circuits and held that a plaintiff may be able to establish an injury in fact for purposes of Article III standing based on an increased risk of future identity theft or fraud stemming from the unauthorized disclosure of the plaintiff's data. 995 F.3d at 300–01. Acknowledging that the inquiry is highly fact specific, *id.* at 302, the Second Circuit in *McMorris* directed district courts to consider three non-exhaustive factors: (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. *Id.* at 303. For the reasons that follow, the Court concludes that Plaintiffs have not met their burden of demonstrating an injury in fact.

Defendant principally argues that Plaintiffs did not suffer an injury in fact because "all of the information about them that could have been accessed in the [malware] attack is publicly available" and, "[t]hus, no private sensitive personal or financial information relating to Plaintiffs ever could have been compromised." (ECF No. 12-1 at 1–2) In support of its motion to dismiss, Defendant attached two affidavits and two exhibits.

Defendant's Software Development Manager, Bradley, S. Zygmunt, avers in an August 11, 2021 affidavit that the extent of information that Defendant maintains concerning Plaintiffs is limited to their names, genders, dates of birth, current and former mailing addresses, and information regarding their vehicles. (ECF No. 12-2 at 2–3) Zygmunt specifically avers that Defendant does not maintain any private or sensitive personal or financial information concerning Plaintiffs, such as their personal identification numbers, Social Security numbers, or driver's license numbers.[5] (*Id*. at 3)

Moreover, Defendant's counsel, Attorney Vogt, avers in an August 12, 2021 affidavit that the PII maintained by Defendant—Plaintiffs' names, addresses, and dates of birth—is accessible in publicly available records on the internet and has been published on the website, www.truthfinder.com. (ECF No. 12-3 at 2) Defendant submitted two exhibits of July 24, 2021 reports created on www.truthfinder.com ("Truthfinder reports"), one with respect to each named Plaintiff—Yankovich and Allen. (ECF No. 12-3 at 3–11) The Truthfinder reports contain personal, occupational, educational, and residential information with respect to each Plaintiff, including, *inter alia*, their names, dates of birth, and current and former mailing addresses. (*Id*.) In combination, Defendant argues that this evidence refutes any allegations which might have otherwise been relied upon to establish an injury in fact. (ECF No. 12-1 at 1–2); (ECF No. 26 at 2)

Plaintiffs respond that the public availability of their information on the internet generally or www.truthfinder.com specifically "does not change the fact that the PII at issue in the [d]ata [b]reach was sensitive" and the unauthorized disclosure of such put Plaintiffs at "an increased risk of identity theft or fraud." (ECF No. 18 at 9–13, 16) Plaintiffs essentially rely upon their allegations

[5] Zygmunt specifically states that Defendant's electronic data system does not facilitate the collection or storage of such information. (*Id*. at 3)

to establish Article III standing. The Court disagrees that Plaintiffs' allegations are sufficient to meet their burden.

Preliminarily, although "plaintiffs are entitled to rely on the allegations in the [p]leading if the evidence proffered by the defendant is immaterial because it does not contradict plausible allegations that are themselves sufficient to show standing," *Carter*, 822 F.3d at 57, such is not the case here. The evidence presented by Defendant is material insofar as it contradicts Plaintiffs' allegations that the PII compromised in the malware attack included Social Security numbers, driver's license numbers, or personal identification numbers or was otherwise confidential, sensitive, and "non-public." It further contradicts Plaintiffs' allegations that public dissemination of the compromised PII increased their risk of identity theft or fraud.[6] Defendant's evidence reveals significant factual problems with Plaintiffs' assertion of subject matter jurisdiction. *McMorris*, 995 F.3d at 302–03. Plaintiffs therefore cannot rely solely upon their contrary allegations to establish standing.[7] *Carter*, 822 F.3d at 57; *Katz*, 872 F.3d at 119.

Notwithstanding, the Court considers the *McMorris* factors looking to both the uncontroverted allegations as well as the evidence provided by Defendant. The first factor—whether the data breach was the result of a targeted attack to obtain the data at issue—favors a

[6] Relatedly, Defendant argues that because the PII at issue was/is publicly available, any increased risk of identity theft or fraud, even if deemed an injury in fact, is not fairly traceable to its conduct. As the Court finds that Plaintiffs have not established an injury in fact, the Court does not take up this issue.

[7] Alternatively, Plaintiffs respond that the Court should find that they have Article III standing because they do not have the benefit of discovery to verify Defendant's contention that it only maintains public information concerning Plaintiffs or that the malware attack did not access Defendant's server that housed data regarding Connecticut residents. It is well established that "precisely because the plaintiff bears the burden of alleging facts demonstrating standing, [the Second Circuit has] encouraged district courts to give the plaintiff ample opportunity to secure and present evidence relevant to the existence of jurisdiction where necessary." *Katz*, 872 F.3d at 121 (citing A*midax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 149 (2d Cir. 2011) (per curiam)) (internal quotation marks omitted). "[E]videntiary production via affidavits, and even limited jurisdictional discovery, may sometimes be appropriate in order to resolve a fact-based Rule 12(b)(1) standing challenge." *Id*. In this case, Plaintiffs did not supplement the record with additional evidence and nor did they pursue limited discovery, even after Defendant notified them that the malware attack did not access the server that housed data regarding Connecticut residents, or through its motion, that the Plaintiffs' PII is publicly available. *Katz*, 872 F.3d at 121. It was Plaintiffs' burden to do so. *Id*.

finding of injury in fact. There is no dispute that Defendant was the victim of a malware attack perpetrated by cybercriminals and that its data was compromised as a result. *See McMorris,* 995 F. 3d at 301 ("[W]here plaintiffs demonstrate that a malicious third party intentionally targeted a defendant's system and stole plaintiffs' data stored on that system, courts have been more willing to find that those plaintiffs have established a likelihood of future identity theft or fraud sufficient to confer standing."). The other two factors—whether any of the compromised data has already been misused; or whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud—favor a finding of no injury in fact.

There are no allegations nor evidence that any of the data compromised by the malware attack has been put to any nefarious purposes, or any purposes at all for that matter. Specifically, there is no allegation that Plaintiffs or any other putative class members have experienced identity theft or fraud, or that their information has been disseminated without their authorization following the malware attack. *See*, *e.g.*, *McMorris,* 995 F.3d at 301–02 (recognizing that plaintiff may establish substantial risk of future injury sufficient to establish injury in fact in context of data breach where some customers of defendant had reported fraudulent charges to their account, even if plaintiffs themselves had not experienced fraudulent activity; or where compromised dataset is available for sale on Dark Web).

As to the third factor, the Second Circuit in *McMorris* observed:

> Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth—especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud. . . . By contrast, less sensitive data, such as basic publicly available information or data that can be rendered useless to cybercriminals does not pose the same risk of future identity theft or fraud to plaintiffs if exposed. So for example, where a plaintiff's credit card number was stolen as part of a data breach, but she promptly cancelled her credit card 'and no other [PII]—such as her birth date or Social Security number—[was] alleged to have been stolen,' we have found that the plaintiff failed to allege 'how she [could] plausibly face a threat of future fraud.'

*Id.* at 302. As discussed above, Plaintiffs' allegations as to the nature of the PII compromised are refuted by Defendant's evidence that it does not collect or store Social Security numbers, driver's license numbers, or personal identification numbers for Connecticut drivers. Defendant has also demonstrated that all of the data they do collect (and which may have been compromised) as to the named Plaintiffs is publicly available. These facts, in combination with the lack of evidence that the server which housed Connecticut driver information was accessed at all during the malware attack, leads to the conclusion that Plaintiffs have not demonstrated that the alleged heightened risk of future injury on which they rely to establish an injury in fact is "certainly impending," or that there is a "substantial risk" that such harm will occur. *Susan B. Anthony List,* 573 U.S. at 158. Indeed, any possible future harm to Plaintiffs is entirely speculative. *See*, *e.g.*, *Mirfasihi v. Fleet Mortg. Corp*., No. 01 C 722, 2007 WL 2066503, at *4 (N.D. Ill. July 17, 2007), *aff'd*, 551 F.3d 682 (7th Cir. 2008) ("Because the information disclosed was already a matter of public record . . . [defendant's] disclosure could not have caused any harm."); *Fus v. CafePress, Inc*., No. 19-CV-06601, 2020 WL 7027653, at *3 (N.D. Ill. Nov. 30, 2020) ("[M]ost of [plaintiff's] information possessed by [defendant] at the time of the hack was publicly available information, such as his billing and shipping address and personal email address. . . . [T]he disclosure of such information does not expose [plaintiff] to a significant risk of identity theft or fraud."); *Jackson v. Loews Hotels, Inc*., No. ED CV 18-827-DMG (JCx), 2019 WL 2619656, at *3–4 (C.D. Cal. Jan. 4, 2019) (finding that the plaintiff suffered no injury-in-fact when "generally publicly available" information such as plaintiff's "full name, email, phone number, and address" was exposed in data breach). *See also McNichols v. GEICO Gen. Ins. Co*., No. 3:20-CV-01497 (KAD), 2021 WL 3079783, at *3 (D. Conn. July 21, 2021) ("[A] plaintiff who suffers no injury in fact has no Article III standing.") (citing *Spokeo*, 578 U.S. at 338).

In sum, on the present record, the Court finds that Plaintiffs did not meet their burden of establishing by a preponderance of the evidence that they suffered an injury in fact.

**Conclusion**

For the foregoing reasons, Defendant's motion to dismiss is GRANTED and this case is DISMISSED without prejudice.[8] The Clerk of the Court is directed to close the case.

**SO ORDERED** at Bridgeport, Connecticut, this 9th day of August 2022.

*/s/ Kari A. Dooley*

KARI A. DOOLEY

UNITED STATES DISTRICT JUDGE

[8] "Article III deprives federal courts of the power to dismiss [the] case with prejudice. . . . As a result, where a case is dismissed for lack of Article III standing, as here, that disposition cannot be entered with prejudice, and instead must be dismissed without prejudice." *Katz*, 872 F.3d at 121 (citation omitted; internal quotation mark omitted).