IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ARTUR PODROYKIN, ***on behalf of himself and all individuals similarly situated,*** **Plaintiff,**	)	
v.	)	**Civil Action No. 1:21-cv-588**
AMERICAN ARMED FORCES MUTUAL AID ASSOCIATION, Defendant.	)	

MEMORANDUM OPINION

At issue in this multi-claim action growing out of a ransomware attack is whether Plaintiff Artur Podroykin has Article III standing to maintain this action. Defendant American Armed Forces Mutual Aid Association ("AAFMAA")'s threshold Motion to Dismiss argues, *inter alia*, that plaintiff has not suffered an injury in fact and therefore does not have standing to sue. The matter has been fully briefed and argued and is ripe for disposition. For the reasons that follow, the Motion to Dismiss must be granted.

I.

Plaintiff is a United States Army veteran and a member of the AAFMAA. Defendant AAFMAA, a mutual aid association for veterans and active duty members of the United States military, sells life insurance policies to its members and provides other services to them. Plaintiff purchased a life insurance policy from defendant in 2010 and, to do so, plaintiff provided defendant with PII which defendant kept on its servers.

In January 2021, a ransomware group known as "DarkSide" gained access to defendant's computer systems and executed a ransomware attack by encrypting troves of highly sensitive files. DarkSide demanded a ransom in exchange for decryption keys which defendant declined

to pay. Plaintiff alleges, on information and belief, that DarkSide, as it has done before, employed a double extortion scheme whereby DarkSide not only encrypted defendant's data locally on defendant's computer, but also extracted the data to place on the dark web.[1] Notably, the Amended Complaint acknowledges that DarkSide no longer maintains websites that are accessible to the public; DarkSide's websites were shut down at least 16 months ago in May or June 2021, just four to five months after the ransomware attack.

Plaintiff initially filed a Complaint on May 10, 2021. On June 23, 2021, defendant filed a Motion to Dismiss the Complaint arguing that plaintiff (i) lacked standing and (ii) failed to state viable claims for relief. On July 19, 2021, an Order issued granting defendant's Motion to Dismiss based on plaintiff's lack of standing. As set forth in the Order, plaintiff lacked standing because (i) plaintiff had not identified any illegitimate use of his PII resulting from the unlawful electronic intrusion into defendant's database and (ii) the attack was a ransomware attack, aimed at locking defendant out of its own systems rather than at stealing PII. 2021 WL 3081139, at *1. The Order afforded plaintiff leave to amend to add a different named plaintiff with standing or otherwise to cure the apparent lack of standing in the Complaint. *Id.*

On October 1, 2021, plaintiff filed an Amended Complaint which names only Artur Podroykin as a plaintiff and does not specifically identify any other plaintiff or member of the putative class. The Amended Complaint does contain, however, additional factual allegations

[1] Defendant disputes this fact. To do so, defendant offers a declaration by William Hardin, a purported expert in information technology, digital forensics, and cyber extortion. Hardin's declaration states that, based on searches of the dark web, none of the information from the January 2021 attack was posted on the dark web. *See* Declaration of William Hardin (Dkt. 39-1).

Because, on a Rule 12(b)(1) challenge to standing, "the district court is entitled to decide disputed issues of fact with respect to subject matter jurisdiction," *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009), it is appropriate to consider the declaration. But as discussed *infra*, whether plaintiff's information was ever on the dark web is not material to the resolution of this Motion. This is so because, regardless of whether plaintiff's PII was on the dark web, plaintiff concedes that it is no longer there, as DarkSide's websites were shut down at least 16 months ago. Thus, for reasons that follow *infra*, plaintiff's claim to standing is too attenuated.

relating (i) to ransomware attacks and double extortion schemes generally and (ii) DarkSide specifically. Thus, the key inquiry is whether any of these allegations, alone or taken together with the rest of the Amended Complaint, confer standing upon plaintiff.

II.

Article III of the Constitution limits federal court jurisdiction to "Cases" and "Controversies," and this limitation is implemented, in part, by standing doctrine. The "irreducible constitutional minimum" of standing consists of three elements: the 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 judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). And "[t]he plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Id.* Where, as here, a "case is at the pleading stage," the Amended Complaint must "allege facts demonstrating" each element "clearly." *Id.* And in "evaluating a class action complaint" standing is analyzed based on allegations "made by the named plaintiffs." *Hutton v. Nat'l Bd. Of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 620 (4th Cir. 2018). The parties' briefing and oral argument focused on whether plaintiff can demonstrate the first element of standing: an injury in fact.

Although the Fourth Circuit has not issued an opinion regarding standing in a case with facts identical to those presented here, two recent Fourth Circuit decisions are instructive and indeed dispositive here. Those decisions are *Beck v. McDonald*, finding no standing, and *Hutton*, finding standing. A careful review of those cases and their comparison to the instant case make clear that the Amended Complaint contains no factual allegations that adequately allege standing.

To begin with, *Beck* was a consolidated appeal of two cases regarding data breaches at a veterans' affairs medical center: the first involved a stolen laptop containing the plaintiffs' PII and the second involved a box of missing documents containing the plaintiffs' PII. 848 F.3d 262, 266 (4th Cir. 2017). The *Beck* plaintiffs, to establish standing, attempted to assert an injury in fact based on an "increased risk of future identity theft" and the "costs of protecting against" identity theft. *Id.* at 273. This attempt to allege standing in *Beck* failed for three reasons.

First, although *Beck* noted a circuit split regarding whether standing can be premised merely on an "increased risk of future identity theft," the Fourth Circuit concluded that the *Beck* plaintiffs failed to demonstrate standing on either side of that split. *Id.* This was so because, absent allegations of actual misuse, a complaint must contain allegations sufficient to show that "the data thief intentionally targeted the personal information compromised in the data breaches." *Id.* at 274. As the *Beck* plaintiffs' complaint lacked such allegations, those plaintiffs' "contention of an enhanced risk of future identity theft" was "too speculative." *Id.* Moreover, allegations that the stolen laptop and documents contained PII were not enough as those allegations alone would require the Fourth Circuit to speculate regarding an "attenuated chain of possibilities" by "assum[ing] that the thief targeted the stolen items for the personal information they contained" and then "select[ed], from thousands of others, the personal information of the named plaintiffs" in an attempt to "use that information to steal their identities." *Id.* at 275. The Fourth Circuit held that this speculative reasoning was an inappropriate basis to establish standing, especially because the alleged data breaches occurred over two-and-a-half years before the Fourth Circuit's decision, decreasing the likelihood of future identity theft. *Id.* at 274-75.

Second, although the Fourth Circuit noted that a "substantial risk" of concrete harm, such as identity theft or other misuse of PII, may confer standing, the *Beck* plaintiffs still did not meet

that standard. *Id.* at 275. This was so because allegations that "33% of health-related data breaches result in identity theft" naturally imply that "over 66%" will "suffer no harm." *Id.* at 275-76. Further, an "organization's offer to provide free credit monitoring" cannot demonstrate that there is a "substantial risk" of concrete harm, lest an organization's "goodwill render [it] subject to suit." *Id.* at 276.

Third, although plaintiffs alleged that they had incurred "the cost of measures to guard against identity theft, including the costs of credit monitoring services," such costs are "self-imposed harms" that cannot confer standing. *Id.* at 276-77.

Here, as in *Beck*, the allegations are insufficient to confer standing upon plaintiff because (i) plaintiff has not alleged misuse of his PII or facts demonstrating that plaintiff's PII was the target of the DarkSide's attack; (ii) plaintiff has not alleged facts sufficient to show a substantial risk of harm; and (iii) plaintiff's costs incurred in mitigating the speculative injury of identity theft were self-imposed harms.

First, because plaintiff concedes that he cannot demonstrate misuse of his PII, *see* Dec. 17, 2021 Tr. at 5:15-17, plaintiff must allege facts sufficient to show that "the data thief intentionally targeted the personal information compromised in the data breaches." *Beck*, 848 F.3d at 274. Absent such allegations, the Fourth Circuit concluded, the claim of standing is "too speculative." *Id.*

Here, although the Amended Complaint states in a conclusory fashion that "PII was targeted and viewed or removed," Am. Compl. ¶ 55, courts are "not bound to accept [a plaintiff's] conclusory allegations regarding the legal effect of the facts alleged." *Labram v. Havel*, 43 F.3d 918, 921 (4th Cir. 1995). And there are no allegations *of fact* sufficient to show such targeting. To be sure, the Amended Complaint alleges that "an unauthorized actor gained

access" to certain systems "and removed and/or viewed certain files." Am. Compl. ¶ 54. And the Amended Complaint contains allegations demonstrating that the hacker in this case, DarkSide, may have used a "double extortion" ransomware attack whereby it placed malware on computers to block the defendant from using or accessing their systems and threatened to sell the locked data on the dark web if ransom demands are not met (and they were not met in this case). *See* Am. Compl. ¶¶ 39-53.[2] But none of those allegations lead to the conclusion that DarkSide was targeting plaintiff's PII, as opposed to other sensitive data. *Cf. Beck*, 848 F.3d at 269 (holding that allegations of theft of data or files containing PII is not enough to confer standing). Further, the Amended Complaint also reveals (i) that nearly two years have passed since the alleged data breach occurred in January 2021 with no indication that plaintiff's PII has been misused or that plaintiff has suffered identity theft and (ii) that even if plaintiff's PII was on the dark web at one point, the PII is on the dark web no longer because DarkSide's websites shut down in May or June 2021, at least 16 months ago. Am. Compl. ¶ 50.

Plaintiff's theory of standing thus requires making analytical jumps by speculating: (1) that DarkSide targeted plaintiff's PII in its ransomware attack; (2) that plaintiff's PII was part of the swath of data encrypted by DarkSide; (3) that DarkSide engaged in a double extortion scheme and placed the stolen swath of data, including plaintiff's PII, on the dark web; (4) that plaintiff's PII was thereafter downloaded by some evil actor in the four to five months before DarkSide's website was shut down; and (5) that the evil actor has been lying in wait, for over 16 months, to steal plaintiff's identity or otherwise misuse the PII. Such an "attenuated chain

[2] As discussed *supra*, this fact is disputed. But even crediting plaintiff's allegations, there is no evidence that DarkSide was targeting plaintiff's PII, and targeting is required by the Fourth Circuit's decision in *Beck*. In any event, even if the stolen data was once on the dark web, plaintiff acknowledges that it has not been on the dark web for at least the past 16 months. Plaintiff's theory of standing thus requires speculating that there will be misuse of the PII, even though there has not yet been misuse and even though the PII is no longer available on the dark web. Such speculation is inappropriate.

cannot confer standing." *Beck*, 848 F.3d at 275 (internal quotation marks omitted).

Second, plaintiff here, like the plaintiffs in *Beck*, has failed to demonstrate a "substantial risk" of concrete harm. *Id.* at 275. To begin with, plaintiff here does not proffer any statistics to allege a high risk of identity theft following a ransomware attack. Although plaintiff alleges that ransomware attacks rose by 62% worldwide and that 10% of all breaches involve ransomware, these allegations do not establish a substantial risk of *identity theft* or other harm as a result of a ransomware attack. Indeed, on that critical question, the Amended Complaint is silent and thereby leaves a missing link between the probability of a ransomware attack and the probability of resulting harm. *Cf. Beck*, 848 F.3d at 275-76 (analyzing statistics relating to the chance that data breach victims "will become victims of identity theft"). And even if plaintiff did allege statistics regarding the chance of identity theft after a ransomware attack, a 33% chance would be insufficient. *Id.*

Quite apart from the absence of any statistics establishing that ransomware attacks lead to identity theft, plaintiff cannot demonstrate a substantial risk of identity theft here because, according to the Amended Complaint, plaintiff's PII is no longer on the dark web, even if it once was. Am. Compl. ¶ 50 ("In May or June 2021, following pressure from U.S. authorities after the Colonial Pipeline hack, DarkSide shut down its public-facing websites."). Given this fact, it is hard to infer that there is a "substantial risk" of concrete harm in the future. *Cf. Beck*, 848 F.3d at 275-76 (holding that a 33% chance of identity theft after a data breach is insufficient to establish a substantial risk of harm). Moreover, just as in *Beck*, the defendant's offer in this case to provide free credit monitoring cannot demonstrate that there is a "substantial risk" of harm, lest defendant's "goodwill render [it] subject to suit." *Id.* at 276.

Third, as in *Beck*, plaintiff's allegations related to the "cost of measures to guard against

identity theft, including the costs of credit monitoring services," are "self-imposed harms" plaintiff "incurred in response to a speculative threat." *Id.* at 276-77. Simply put, plaintiff's argument in this regard is "merely a repackaged version" of plaintiff's other arguments regarding standing and fails for the same reasons. *Id.* at 276 (internal quotation marks and citation omitted).

The conclusion that plaintiff lacks standing is supported by the Fourth Circuit's decision in *Hutton*, which found standing because the *Hutton* plaintiffs had demonstrated actual misuse. Specifically, the *Hutton* plaintiffs, unlike the *Beck* plaintiffs and unlike plaintiff here, alleged that they had "already suffered actual harm in the form of identity theft and credit card fraud" because their personal information had been used "to open Chase Amazon Visa credit card accounts without their knowledge or approval." *Hutton*, 892 F.3d at 622. Thus, in *Hutton*, there was no need to speculate on whether substantial harm will befall the plaintiffs because substantial harm had already occurred. *Id.* Unlike in *Hutton*, plaintiff here does not allege that he "already suffered actual harm in the form of identity theft and credit card fraud" due to fraudulent credit lines or any other form of actual misuse. 892 F.3d at 622. Thus, plaintiff here, unlike in *Hutton*, is "speculat[ing] on whether substantial harm will befall." *Id.*

Plaintiff proffers several other theories of standing, none of which is persuasive. First, plaintiff argues that plaintiff has experienced significant emotional distress sufficient to confer standing. But plaintiff has not demonstrated any substantial risk of identity theft that could plausibly lead to emotional distress. Any emotional distress experienced by plaintiff in this case therefore rests on an attenuated and speculative risk that cannot support standing. Indeed, the *Beck* court flatly rejected the "claim that emotional upset and fear of identity theft and financial fraud resulting from . . . data breaches are . . . sufficient to confer Article III standing" *Beck*, 848

F.3d at 272, 276 (internal quotation marks and citation omitted).

Second, plaintiff alleges an overpayment or benefit-of-the-bargain injury. Plaintiff's theory is that one component of defendant's services is the explicit and implicit promise to protect PII, and that had plaintiff known that defendant could not protect plaintiff's PII, plaintiff would have paid less for services. For support, plaintiff cites two cases: *Carlsen v. Gamestop, Inc.*, 833 F.3d 903 (8th Cir. 2016) and *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp 3d 447 (D. Md. 2020). But the Fourth Circuit has never held that an overpayment or benefit-of-the-bargain theory in a data breach context is sufficient to confer standing. And even courts willing to entertain this theory of standing "consistently reject[]" this theory in "data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach." *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (internal quotation marks and citation omitted). Although plaintiff asserts that, had he known that AAFMAA was vulnerable to a cyber-attack, he would not have "purchased or would have paid less for" the insurance policy, plaintiff nowhere claims that the actual value of the insurance policy has decreased. Am. Compl. ¶ 95. Given this, plaintiff's reliance on *Marriott* and *Carlsen* is misplaced; plaintiff here, unlike the *Marriott* and *Carlsen* plaintiffs, has failed to make allegations that the data breach diminished the value of his insurance. *Marriott*, 440 F. Supp. 3d at 466; *accord Carlsen*, 833 F.3d at 909 (noting that such an allegation was made).

Finally, plaintiff argues that his PII's value has been diminished, thereby conferring standing. But to begin with, many courts have "routinely rejected the proposition that an individual's personal identifying information has an independent monetary value." *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016); *see also Willingham v. Glob.*

Payments, Inc., 2013 WL 440702, at *7 (N.D. Ga. Feb. 5, 2013) ("PII does not have an inherent monetary value."). And in any event, even courts that are willing to consider diminution in the value of PII as a basis for standing do so when there are allegations of some concrete injury, such as "lower credit scores" or "fraudulent accounts and tax returns . . . filed in [plaintiff's] name[.]" *Marriott*, 440 F. Supp. 3d at 462. Here, of course, plaintiff cannot even allege that his PII has been misused, and so plaintiff here cannot argue that the value of his PII has been diminished.

III.

In sum, the Amended Complaint does not allege any facts sufficient to confer standing on plaintiff. Plaintiff's theories of standing all fail because the Amended Complaint contains no allegations of targeting or of a substantial risk of misuse, and in any event acknowledges that plaintiff's PII is no longer available on the dark web. Because plaintiff does not have standing, it is unnecessary to consider defendant's argument that the Amended Complaint fails to state a claim upon which relief can be granted. Accordingly, defendant's Motion to Dismiss pursuant to Rule12(b)(1) must be granted and plaintiff's Amended Complaint must be dismissed.

An appropriate Order will issue.

The Clerk is directed to send a copy of this Memorandum Opinion to all counsel of record and to place this matter among the ended causes.

Alexandria, Virginia
October 11, 2022

/s/
T. S. Ellis, III
United States District Judge