

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

DAVID STEWART,

*Plaintiff,*

v.

FRANK KENDALL, *Secretary of the Air  
Force, in his official capacity, et al.,*<sup>1</sup>

*Defendants.*

Case No. 1:21-cv-1387-RCL

**MEMORANDUM OPINION**

Plaintiff Major David Stewart sued defendants Frank Kendall, in his official capacity as Secretary of the Air Force, and Daniel Hokanson, in his official capacity as Chief of the National Guard Bureau, for alleged violations of the Privacy Act involving a leak of his private medical information to a member of Congress. Defendants moved to dismiss for lack of subject matter jurisdiction and failure to state a claim. Defs.'s Mot., ECF No. 3. Plaintiff responded, Pl.'s Resp., ECF No. 6, and defendants replied, Defs.'s Rep., ECF No. 9. For the reasons explained below, this Court will **GRANT** defendants' motion to dismiss for lack of subject matter jurisdiction and will **DISMISS** plaintiff's claim by separate Order.

**I. BACKGROUND**

Plaintiff was a physician assistant with the 129th Medical Group in the California Air National Guard ("CA ANG"). Compl. ¶¶ 1 & 7, ECF No. 1. Lieutenant Colonel Sean Haugh, the Chief of Clinical Services, was one of plaintiff's supervisors. *Id.* ¶ 7. Plaintiff alleges that Lt. Col. Haugh "never particularly cared for" him. *Id.* ¶ 10. During his service with the CA ANG, plaintiff

---

<sup>1</sup> Pursuant to Fed. R. Civ. P. 25(d), a public officer's successor is automatically substituted as a party. Frank Kendall is accordingly substituted as Defendant in place of former Acting Secretary John Roth.

was in a motor vehicle accident where “he sustained substantial medical injuries and developed a resultant psychiatric condition.” *Id.* ¶ 8. Following this accident, plaintiff was placed on temporary disability status. *Id.*

Air Force Instruction, a set of directives for the United States Air Force, required that plaintiff obtain a medical waiver to continue serving with the CA ANG. *Id.* ¶ 9. To obtain this medical waiver, plaintiff authorized the release of his medical records to the 129th Medical Group for the sole purpose of this assessment. *Id.* Lt. Col. Haugh sought to have plaintiff involuntarily medically separated because of his psychiatric condition. *Id.* ¶ 10. Lt. Col. Haugh eventually began to “circumvent[] proper channels” in his quest to process plaintiff for separation, including disclosing all of plaintiff’s treatment providers and diagnoses to each of his treating physicians. *Id.* ¶ 10. Plaintiff accordingly filed a complaint with the California National Guard Inspector General’s office. *Id.* ¶ 10–11. After an investigation, plaintiff was transferred to another medical group away from Lt. Col. Haugh. *Id.* ¶ 11.

The now “infuriated” Lt. Col. Haugh’s vendetta continued. *Id.* ¶ 12. Convinced plaintiff had fraudulently enlisted in the CA ANG, Lt. Col. Haugh raised concerns with unit leadership, but leadership did not act on his allegations. *Id.* Unsatisfied, Lt. Col. Haugh accessed plaintiff’s medical records in the Aeromedical Information Management Waiver Tracking System (“AIMWTS”)<sup>2</sup> and downloaded thirteen pages of psychiatric counselling sessions and plaintiff’s medical waiver narrative. *Id.* ¶ 13. Armed with these records, Lt. Col. Haugh hand-delivered them to Congresswoman Anna Eshoo’s office on October 15, 2018. *Id.* ¶ 14.

After Eshoo’s staff immediately contacted the CA ANG, Brigadier General Jeffrey Magram ordered a Command Directed Investigation (“CDI”). *Id.* ¶ 15–18. It was during a CDI

---

<sup>2</sup> AIMWTS is a database controlled by the Air Force. Compl. ¶ 13.

interview on May 14, 2019, that plaintiff first learned of the breach of his private medical records. *Id.* The CDI's Report of Investigation ("ROI") concluded by a preponderance of the evidence that Lt. Col. Haugh violated the Privacy Act. *Id.* ¶ 19.

Plaintiff was distraught by the unlawful distribution of his private medical records and "sought mental health treatment to cope." *Id.* ¶ 20. Because he "no longer felt comfortable seeking any treatment that was remotely connected to the military," plaintiff paid for mental health treatment with his own personal finances as opposed to receiving treatment from the military. *Id.* Plaintiff also "stopped pursuing his goal of becoming a flight surgeon and assumed an ANG staff officer position outside of medicine" because of his disillusionment with the military medical profession." *Id.* ¶ 21.

Plaintiff initially attempted to file his complaint with this Court on May 14, 2021, attached to a motion for leave to file under seal. *Stewart v. Roth*, No. 21-mc-54 (UNA) (D.D.C. May 17, 2021), ECF Nos. 1-1 & 1-3. On May 17, 2021, Chief Judge Beryl Howell denied plaintiff's motion to for leave to file under seal. Order, *Stewart v. Roth*, No. 21-mc-54 (UNA) (D.D.C. May 17, 2021), ECF No. 1. Plaintiff filed an unsealed complaint on May 20, 2021. Compl., ECF No. 1.

Plaintiff's complaint brings claims against the Air Force, which maintained the AIMWTS database where his medical records were kept, and the National Guard Bureau ("NGB"), of which Lt. Col. Haugh was an officer. Compl. ¶ 3, 22-26. He seeks reimbursement for the thousands of dollars he spent on "out-of-pocket" mental health treatment, as well as lost wages from attending his doctor's appointments. *Id.* ¶ 26.

Defendants moved to dismiss pursuant to both Federal Rules of Civil Procedure 12(b)(1) and (b)(6). Defs.'s Mot., ECF No. 3. Defendants' argument hinges on one point: that plaintiff failed to plead actual damages as required by the Privacy Act. They contend that plaintiff's mental

distress is not cognizable under the Privacy Act. Defs.'s Mot. 6. They further contend that plaintiff lacks standing to recover for his out-of-pocket medical costs because he did not plausibly allege a substantial risk that his medical records would be again accessed without authorization. *Id.* Defendants' motion is now ripe.

## II. LEGAL STANDARDS

### A. Motion To Dismiss For Lack Of Subject Matter Jurisdiction

A federal court is a court of limited jurisdiction, possessing "only that power authorized by Constitution and statute." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). Before a court may "proceed at all in any cause" it must ensure that it possesses subject matter jurisdiction. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998) (quoting *Ex parte McCardle*, 74 U.S. (7 Wall.) 506, 514 (1868)). The party invoking federal jurisdiction—in this case, plaintiff—bears the burden of establishing jurisdiction. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). A court considering jurisdiction accepts the factual allegations in the complaint as true. *Info. Handling Servs., Inc. v. Def. Automated Printing Servs.*, 338 F.3d 1024, 1029 (D.C. Cir. 2003). But because a Rule 12(b)(1) motion concerns a court's power to hear a claim, courts must more closely scrutinize plaintiff's factual claims when resolving a 12(b)(1) motion than when resolving a 12(b)(6) motion for failure to state a claim. *Grand Lodge of Fraternal Ord. of Police v. Ashcroft*, 185 F. Supp. 2d 9, 13–14 (D.D.C. 2001).

### B. Motion To Dismiss For Failure To State A Claim

To survive a motion to dismiss under Rule 12(b)(6), a "complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The factual content included in the complaint must allow "the court to draw the reasonable

inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. Courts resolving a Rule 12(b)(6) motion assume “the truth of all well-pleaded factual allegations in the complaint and construe[] reasonable inferences from those allegations in the plaintiff’s favor,” but courts are “not required to accept the plaintiff’s legal conclusion as correct.” *Sissel v. Dep’t Health & Human Servs.*, 760 F.3d 1, 4 (D.C. Cir. 2014).

### **C. Claims Under The Privacy Act**

The Privacy Act “contains a comprehensive and detailed set of requirements for the management of confidential records held by Executive Branch agencies.” *FAA v. Cooper*, 566 U.S. 284, 287 (2012). To maintain a claim under the Privacy Act, a plaintiff must allege that (1) an agency violated a provision of the act, (2) the agency’s violation was intentional or willful, and (3) the violation had an “adverse effect” on the plaintiff “in the form of actual damages.” *Chichakli v. Tillerson*, 882 F.3d 229, 233 (D.C. Cir. 2018); 5 U.S.C. § 552a(g). “Actual damages,” as used in the Privacy Act, only encompasses “damages for proven pecuniary loss.” *Cooper*, 566 U.S. at 298. “[D]amages for mental or emotional distress” are not sufficient to maintain a Privacy Act claim. *Id.* at 287.

## **III. DISCUSSION**

### **A. This Court Lacks Subject Matter Jurisdiction Because Plaintiff Has Failed To Plausibly Allege “Actual Damages”**

This Court lacks subject matter jurisdiction, because plaintiff’s emotional damages are insufficient to waive sovereign immunity and plaintiff lacks standing for his proffered pecuniary damages, which *would* waive sovereign immunity. Plaintiff alleges that this Court has jurisdiction over his action pursuant the Privacy Act. Compl. ¶ 4. In claims against the federal government, “sovereign immunity shields the federal government and its agencies from suit” and a court must dismiss a claim for lack of subject matter jurisdiction “[a]bsent a waiver”. *FDIC v. Meyer*, 566

U.S. 284, 304 (2012). The Privacy Act provides a waiver of sovereign immunity, but the waiver is limited in scope: the Act only waives sovereign immunity for “actual damages.” *Cooper*, 566 U.S. at 291; 5 U.S.C. § 552(g)(1)(D), (g)(4)(A). These “actual damages,” in turn, must be pecuniary or economic in nature. *Cooper*, 566 U.S. at 298. Put simply, for this Court to have subject matter jurisdiction, the United States must have consented to being sued, and the United States only consented to being sued under the Privacy Act for pecuniary damages. Because plaintiff lacks standing for his pecuniary damages, the Privacy Act cannot serve as a waiver of sovereign immunity and this Court lacks subject matter jurisdiction.

Plaintiff raises two types of damages in his complaint. First, he alleges that he was “severely distraught” by the Privacy Act violation in question. Compl. ¶ 20. But the Privacy Act does not permit damages for “mental or emotional distress.” *Cooper*, 566 U.S. at 304. “Accordingly, the Act does not waive the Federal Government’s sovereign immunity from liability for such harms.” *Id.* This Court lacks subject matter jurisdiction over plaintiff’s claims of emotional injury.

Second, plaintiff *does* proffer pecuniary damages that would waive the government’s sovereign immunity, but lacks standing for these claims. Plaintiff claims he suffered pecuniary losses from out-of-pocket payments for medical expenses he incurred after foregoing military medical assistance and from “lost wages to attend these doctor’s appointments.”<sup>3</sup> While these pecuniary damages, if plausibly alleged, would serve to waive the government’s sovereign immunity under the Privacy Act, plaintiff runs into a different subject matter jurisdiction issue.

---

<sup>3</sup> For the first time in his response, plaintiff also alleges pecuniary harm in the form of diminished employment opportunities—e.g. that the breach “forced him to take alternative paths” to avoid another breach. Pl.’s Resp. 6. But his complaint only specifically alleges as damages out-of-pocket mental health treatment and lost wages. Compl. ¶ 26. As defendants note, a complaint “may not be amended by the briefs in opposition to a motion to dismiss.” Defs.’s Resp. 3 (quoting *Coleman v. Pension Benefit Guar. Corp.*, 94 F. Supp. 2d 18, 24 n.8 (D.D.C. 2000)). The Court therefore will not address these damages but notes they would likely suffer from similar standing issues.

These damages fail to fulfill the injury-in-fact requirement of Article III standing, and so this Court lacks subject matter jurisdiction over these claims as well.

To maintain any claim in federal court, a plaintiff must make three showings: (1) that he has suffered an injury-in-fact that is “actual or imminent, not ‘conjectural’ or ‘hypothetical’”; (2) that the injury was “fairly traceable to the challenged action of the defendant”; and (3) that it is likely that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560. An injury-in-fact must be “concrete, particularized, and, most importantly for our purposes, ‘actual or imminent’ rather than speculative.” *Attias v. Carefirst, Inc.*, 865 F.3d 620, 626 (D.C. Cir. 2017) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 229 (2016)).

As plaintiff appears to concede, military-associated mental health treatment would have been paid for by the military itself. Compl. ¶ 20. But plaintiff explains that he “no longer felt comfortable seeking any treatment that was remotely connected to the military” and accordingly began to pay for treatment on his own. Compl. ¶ 20. Defendants characterize this as a “voluntarily assumed harm” insufficient to confer standing. Defs.’s Mot. 7.

Mitigation costs incurred to prevent future injury can qualify as actual damages and satisfy the injury-in-fact standing requirement only if there is at least a substantial risk of future harm. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013). Because plaintiff alleges that he sought outside treatment to avoid a “repeat privacy breach,” Pl.’s Resp. 9, plaintiff’s pecuniary mitigation costs can satisfy the injury-in-fact requirement if there was a substantial risk of a future privacy breach. But plaintiff fails to plausibly allege that Lt. Col. Haugh’s breach of his personal information was anything other than an isolated incident unlikely to reoccur.

Plaintiff brings no allegations about the potential threat of a repeat breach beyond noting that the “actual breach demonstrates the ease of accessing the Air Force database and greatly

increases the likelihood of a repeat privacy breach.” Pl.’s Resp. 9. The mere fact that a breach happened in the past does not mean it is likely to happen again in the future. The notion that *another* bad actor with access to AIMWTS and a personal vendetta against plaintiff will again download his medical records without authorization and attempt to leak them is a paradigmatic speculative harm based on a “highly attenuated chain of possibilities.” *Clapper*, 568 U.S. at 410. Plaintiff “cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.” *Id.* at 402.

The case law he cites to support his theory of standing is similarly inapposite. Plaintiff relies heavily on two cases that found a substantial risk of future harm based on a data breach. *See* Pl.’s Resp. 6–9. In *Attias*, a health insurance provider “suffered a cyberattack” in which customers’ personal information was stolen. 865 F.3d at 622. The Circuit found that the plaintiffs plausibly alleged that they “face a substantial risk of identity theft as a result of [the provider’s] alleged negligence” because the breach “exposed [their] social security and credit card numbers” to an intruder. *Id.* at 627–28. Because the breach had already happened, “an unauthorized party had already accessed” personal data and it was “plausible . . . to infer that this party has both the intent and the ability to use that data for ill.” *Id.* at 628. Similarly, in *In re United States Office of Personnel Management Data Security Breach Litigation* (“*In re OPM*”), plaintiffs bringing a Privacy Act suit made a nearly identical claim to *Attias*: that a widespread data breach which exposed their personal information (including Social Security numbers, birth dates, residency details, and fingerprints) made them susceptible to the risk of future fraud and identity theft. 928 F.3d 42, 58–59 (D.C. Cir. 2019). The Circuit agreed and found that the costs incurred by purchasing credit-monitoring services, along with other mitigation costs, qualified as an injury-in-fact. *Id.* at 60.

But plaintiff here does not allege that because of the Privacy Act violation his personal information is currently in the hands of a malicious actor seeking to steal his identity. He does not allege that he is at a substantial risk of future identity theft or other damages because of the breach. Instead, he alleges that he is at risk of a “repeat privacy breach.” Pl.’s Resp. 9. This alleged threat of future harm differs greatly from the harm in *Attias* and *In re OPM*. Neither court found substantial risk of a future repeat breach.

Because plaintiff has failed to allege an injury-in-fact sufficient to confer Article III standing or the “actual damages” required by the Privacy Act to waive the government’s sovereign immunity, this Court does not have subject matter jurisdiction. Accordingly, the motion to dismiss under Rule 12(b)(1) will be granted.<sup>4</sup>

#### IV. CONCLUSION

For the above-mentioned reasons, this Court will **GRANT** defendants’ motion to dismiss for lack of subject matter jurisdiction by separate order.

Date: Jan. 3, 2022  
December \_\_, 2021

Royce C. Lamberth  
Hon. Royce C. Lamberth  
United States District Judge

---

<sup>4</sup> Defendants also argue that plaintiff’s claims should be dismissed for failure to state a claim and as untimely. Defs.’s Repl. 1, 7. The Court need not reach these issues because it dismisses for other reasons.