IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DENISE NEMETH-GREENLEAF, *et al.*, Plaintiffs, v. UNITED STATES OFFICE OF PERSONNEL MANAGEMENT, *et al.*, Defendants.	Case No. 1:25-cv-00407-CRC Judge Christopher R. Cooper

DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' COMPLAINT

Defendants—the U.S. Office of Personnel Management ("OPM"); Charles Ezell, in his official capacity as Acting Director of OPM; Amanda Scales, in her official capacity as Chief of Staff of OPM; Brian Bjelde, in his official capacity as Senior Advisor of OPM; The U.S. Department of the Treasury ("Treasury"); Scott Bessent, in his official capacity as Secretary of the Treasury; and Gregory Barbaccia, in his official capacity as the Federal Chief Information Officer ("FCIO")[1]—move the Court to dismiss this action for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) and for failure to state a claim upon which relief can be granted under Federal Rule of Civil Procedure 12(b)(6).

[1] Plaintiffs note that Gregory Barbaccia is the "CIO for OPM . . . and oversees OPM's software systems and cybersecurity policies and practices." Compl. ¶ 16, ECF No. 1. Gregory Barbaccia's current role as FCIO, however, is organizationally located within the Office of Management and Budget. *See* 44 U.S.C § 3602(a)-(b) (the Administrator of the Office of Electronic Government referenced in the statute is informally known as the FCIO).

Dated: May 19, 2025

Respectfully submitted,

YAAKOV M. ROTH
Acting Assistant Attorney General

MARCIA BERMAN
Assistant Director, Federal Programs Branch

/s/ Pierce J. Anon
PIERCE J. ANON (N.Y. Bar # 6184303)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 305-7573
Email: pierce.anon@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DENISE NEMETH-GREENLEAF, *et al.*, Plaintiffs, v. UNITED STATES OFFICE OF PERSONNEL MANAGEMENT, *et al.*, Defendants.	Case No. 1:25-cv-00407-CRC Judge Christopher R. Cooper

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Other Authorities

INTRODUCTION

In this case, Plaintiffs allege that the U.S. Office of Personnel Management ("OPM") and the U.S. Department of the Treasury ("Treasury") have impermissibly allowed employees, detailees, and affiliates of the U.S. Department of Government Efficiency Service ("USDS" or "DOGE"), to access their personal security information ("PSI") in violation of the Privacy Act of 1974. Plaintiffs claim not only that these individuals were not Government employees but also that there was no lawful or legitimate need for such information. Plaintiffs' Complaint characterizes this alleged disclosure of information as akin to giving "hackers" access to their information. Compl. ¶ 4, ECF No. 1. Plaintiffs seek actual and statutory damages, as well as injunctive, equitable, and declaratory relief, along with prejudgment interest and associated litigation costs.

Plaintiffs' claims are sensational, conclusory, and threadbare. Plaintiffs lack standing because they do not sufficiently allege any cognizable Article III injury. For one thing, a statutory violation, i.e., unauthorized access to Plaintiffs' information, does not by itself create standing. Plaintiffs have alleged no public disclosure of any information accessed by DOGE-affiliated personnel, nor have they claimed concrete, non-speculative, particularized harm resulting from the alleged unauthorized access.

Plaintiffs also fail to state a claim for which relief can be granted. Plaintiffs' alleged harms are not cognizable under the Privacy Act. In short, the Privacy Act requires that Plaintiffs plead pecuniary harm. Apart from the alleged pecuniary harm from purchasing identity theft mitigation services, Plaintiffs fail to do so. And their attempt to create pecuniary harm by buying identity theft prevention services also fails because there is no substantial risk of future harm under the facts of the complaint to justify that expenditure. Accordingly, Plaintiffs' Complaint should be dismissed.

BACKGROUND

I. The Privacy Act

The Privacy Act of 1974, 5 U.S.C. § 552a, "was designed to provide individuals with more control over the gathering, dissemination, and accuracy of agency information about themselves." *Greentree v. U.S. Customs Serv.*, 674 F.2d 74, 76 (D.C. Cir. 1982). The Act was Congress's response to "a growing awareness that governmental agencies were accumulating an ever-expanding stockpile of information about private individuals that was readily susceptible to both misuse and the perpetuation of inaccuracies that the citizen would never know of, let alone have an opportunity to rebut or correct." *Londrigan v. FBI*, 670 F.2d 1164, 1169 (D.C. Cir. 1981).

The Privacy Act creates procedures "to give the individual some control over the ways in which Federal executive agencies handle[] . . . personal information at every stage of the information process." Comm'n on Fed. Paperwork, *Privacy and Confidentiality: Issues in Information Sharing*, 21 (1977). To that end, the Act imposes burdens on federal agencies and creates rights for individuals when agencies collect, maintain, use, and disseminate "records." The Act defines "record" to include "any item, collection, or grouping of information about an individual that is maintained by an agency." 5 U.S.C. § 552a(a)(4).

If an agency maintains the records it collects such that information can be retrieved "by the name of [an] individual or by some identifying number, symbol, or other identifying particular"—a "system of records"—additional responsibilities obtain. *Id.* § 552a(a)(5). Among other things, an agency may not disclose records contained in a system of records except with the consent of the individual to whom the record pertains, or pursuant to one of twelve exceptions. *Id*. § 552a(b). One of those exceptions allows disclosure of covered records to "those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *Id*. § 552a(b)(1).

The Act does not specifically provide a remedy for violations of its prohibition on disclosure. Instead, that prohibition is made enforceable through a catch-all remedial provision

applicable when the agency "fails to comply with any other provision of this section"—that is, any provision other than those relating to accessing and correcting records. *Id.* § 552a(g)(1)(D). If the agency's failure has "an adverse effect on an individual," the affected person may bring a civil suit in federal district court. *Id.* And if that failure "was intentional or willful," the plaintiff may obtain attorney's fees and the greater of the plaintiff's actual damages or $1,000. *Id.* § 552a(g)(4).

II. The United States DOGE Service And Related Executive Orders

On January 20, 2025, President Trump signed Executive Order 14,158, which directs changes to the previously established U.S. Digital Service designed to implement the President's agenda of "improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." 90 Fed. Reg. 8441, § 4 ("USDS EO"). The USDS EO also redesignated the U.S. Digital Service as the U.S. Department of Government Efficiency Service, or U.S. DOGE Service. *Id.* § 3(a). It established a "U.S. DOGE Service Temporary Organization" in the Executive Office of the President under 5 U.S.C. § 3161, which will terminate on July 4, 2026. USDS EO § 3(b). The USDS EO requires agency heads to establish in their respective agencies a USDS team of at least four agency employees. *Id.* § 3(c).

The USDS EO directs USDS to collaborate with Executive agencies to modernize the technology and software infrastructure of the federal government, to increase efficiency and productivity, as well as ensure data integrity. USDS EO § 4. Regarding Treasury, the need to modernize and ensure data integrity is uniquely critical: the Government Accountability Office ("GAO") has identified "problems in accounting for transactions between federal agencies," resulting in potentially improper payments totaling approximately $2.7 trillion dollars. *See* GAO Report, "Financial Statement Audit: Bureau of the Fiscal Service's FY22 Schedules of the General Fund" (March 30, 2023), *available at* https://perma.cc/JJ6R-S2BG. And as to OPM, GAO has identified 16 "priority recommendations" involving "preventing improper payments," "improving payroll data," and "strengthening IT security and management." *See* GAO Report, "Priority Open Recommendations: Office of Personnel Management" (May 28, 2024) at 1-2, *available at*

https://perma.cc/TQA8-M2NS (last visited Apr. 3, 2025) (capitalization and bold removed). GAO stated that "[f]ully implementing these open recommendations could significantly improve both OPM's operations and its efforts to assist federal agencies in addressing various human capital management issues." *Id*. at 1.

To accomplish its objectives, the USDS EO directs USDS to work with relevant agency heads, and vice versa, to ensure USDS has access to "unclassified agency records, software systems, and IT systems" to the "extent consistent with law[.]" USDS EO § 4(b). At all times, the USDS EO instructs, USDS must "adhere to rigorous data protection standards." *Id.*

III. Plaintiffs' Claims

Plaintiffs—five individuals employed by the federal Government—filed suit on February 11, 2025, claiming that Defendants OPM and Treasury have engaged in an unlawful and ongoing disclosure of their personal information in violation of the Privacy Act. Compl. ¶ 2. Such information allegedly includes their full names, addresses, social security number, driver's license, passport number, personal health information, medical records, and financial account information ("Personal Sensitive Information" or "PSI"). *Id.* Plaintiffs claim that they were made aware of the supposed breaches of their PSI from "media reports[,]" and in response, they claim to have purchased varying forms of identity theft protection. *Id*. ¶¶ 19-23.

Plaintiffs allege that both OPM and Treasury permitted unlawful access to persons not employed by the government. They aver that OPM impermissibly disclosed sensitive information through its Enterprise Human Resources Integration ("EHRI") program that manages access to the electronic Official Personnel Folder ("eOPF") for federal employees, *id*. ¶¶ 26-29, 31, and that Treasury disclosed PSI as its Bureau of the Fiscal Service ("BFS") collects and maintains a wide variety of sensitive information in its handling of federal employees' salaries, *id*. ¶¶ 17, 25. Plaintiffs allege that the Secretary of the Treasury, Scott Bessent, personally improperly granted DOGE-affiliated individuals full access to the BFS data and the computer systems that house such data, which includes Plaintiffs' PSI. *Id*. ¶ 34. Plaintiffs claim that DOGE team members within

agencies that were given access to PSI located at Treasury and OPM had not obtained security clearances, taken the required annual Cyber Security and Privacy Awareness training, and did not access the information for a legitimate purpose. *Id*. ¶¶ 34, 37. They further claim that Elon Musk was not a federal government employee at the time of the alleged breach. *Id*. ¶ 32.

The Complaint goes on to enumerate Plaintiffs' purported harms. Plaintiffs assert that they were harmed because they "have no assurance that their PSI will receive the protection that federal law affords" and that permitting this kind of access puts Plaintiffs at risk, making them "vulnerable to fraud, cyber-attack, and actual theft." *Id*. ¶¶ 49-51. And that as a result, Plaintiffs will continue to suffer damages, "including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress." *Id.* ¶ 53. More specifically, Plaintiffs allege that they have suffered, "or are at risk of suffering from": (1) the inability to determine how their PSI is used; (2) the "compromise, publication, and/or theft" of their PSI and that of their family members; (3) out of pocket costs associated with prevention of possible PSI theft; (4) "lost opportunity cost associated with effort expended" from addressing any consequences from possible breaches; (5) continued risk to their PSI; (6) and the current and future costs "in terms of time, effort, and money that will be expended to monitor, prevent, detect, contest, and repair the impact of the compromised PSI data." *Id*.

Plaintiffs request actual and statutory damages, as well as injunctive, equitable, and declaratory relief, and associated litigation costs. *Id*. ¶¶ 19-23. Plaintiffs also seek to certify a proposed class of current, former, and prospective government employees who allegedly had their PSI impermissibly disclosed. *Id.* ¶¶ 54-66.

STANDARD OF REVIEW

I. Rule 12(b)(1)

Federal courts are courts of "limited subject-matter jurisdiction" and have the power "to decide only those cases over which Congress grants jurisdiction." *Al-Zahrani v. Rodriguez*, 669 F.3d 315, 317 (D.C. Cir. 2012) (citing *Micei Int'l v. Dep't of Commerce*, 613 F.3d 1147, 1151 (D.C.

Cir. 2010)). "Absent subject-matter jurisdiction over a case, the court must dismiss it." *Leopold v. Manger*, 630 F. Supp. 3d 71, 76 (D.D.C. 2022). To survive a Rule 12(b)(1) motion, the party asserting subject matter jurisdiction—here Plaintiffs—bear "the burden of establishing it." *Jenkins v. Howard Univ.*, 123 F.4th 1343, 1347 (D.C. Cir. 2024) (quoting *Daimler Chrysler Corp. v. Cuno*, 547 U.S. 332, 342 n.3 (2006)).

II. Rule 12(b)(6)

Defendants also move to dismiss under Federal Rule of Civil Procedure 12(b)(6) for Plaintiffs' failure to state a claim upon which relief can be granted. The standard under Rule 12(b)(6) is a familiar one, in which a plaintiff must allege "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)). In other words, Rule 12(b)(6) "tests the legal sufficiency" of a plaintiff's claims, and dismissal is warranted where a plaintiff can prove "'no set of facts in support of his claim which would entitle him to relief.'" *Browning v. Clinton*, 292 F.3d 235, 242 (D.C. Cir. 2002) (quoting *Conley v. Gibson*, 355 U.S. 41, 45-46 (1957)). In supporting their claims, plaintiffs must go beyond "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements" as such barebones pleadings "do not suffice." *Ashcroft*, 556 U.S. at 678.

Movants—here Defendants—bear the burden of establishing that a Rule 12(b)(6) dismissal is appropriate. *Postal Police Officers Ass'n v. United States Postal Serv.*, 719 F.3d 56, 61 (D.D.C. 2024). In reviewing a motion to dismiss, the Court takes "the operative complaint's well- pleaded factual allegations as true and draw[s] all reasonable inferences in the [plaintiff's] favor." *N. Am. Butterfly Ass'n v. Wolf*, 977 F.3d 1244, 1249 (D.C. Cir. 2020). At the same time, however, courts "need not accept inferences drawn by a plaintiff if those inferences are unsupported by facts alleged in the complaint, nor must the Court accept a plaintiff's legal conclusions." *Arabzada v. Donis*, 725 F. Supp. 3d 1, 9 (D.D.C. 2024) (citing *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 913 (D.C. Cir. 2015)).

ARGUMENT

I. Plaintiffs Lack Standing

Standing is a central component of Article III's case-or-controversy requirement and demands that plaintiffs have "a personal stake in the outcome of the controversy [so] as to warrant his invocation of federal-court jurisdiction." *Warth v. Seldin*, 422 U.S. 490, 498 (1975) (citation omitted). At its "irreducible constitutional minimum," the doctrine requires a plaintiff, as the party invoking the Court's jurisdiction, to establish three elements: (1) a concrete and particularized injury-in-fact, either actual or imminent, (2) a causal connection between the injury and defendants' challenged conduct, and (3) a likelihood that the injury suffered will be redressed by a favorable decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). The party invoking federal court jurisdiction "bears the burden of establishing each of those elements." *Hecate Energy LLC v. FERC*, 126 F.4th 660, 665 (D.C. Cir. 2025).

A. Plaintiffs Fail To Allege A Cognizable Injury-In-Fact

1. Plaintiffs' Alleged Injuries Are Not Concrete Harms

An injury-in-fact must have a "close relationship" to a "harm traditionally recognized as providing a basis for a lawsuit in American courts[.]" *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340-341 (2016)). While Congress "may elevate harms that exist in the real world before Congress recognized them to actionable legal status," at the same time, Congress "may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." *Id.* at 426 (citations and quotations omitted). Congress may create "a statutory prohibition or obligation and a cause of action," but it may not override Article III's injury requirement. *Id.*; *see also Doe v. OPM*, No. 25-cv- 234, 2025 WL 513268, at *5 (D.D.C. Feb. 17, 2025) ("[N]ot every statutory violation results in the type of concrete injury-in-fact sufficient to support Article III standing."). The need for an independent Article III injury is particularly important when considering intangible forms of injury, like the ones Plaintiffs assert in this case.

Plaintiffs proceed under varying theories of injury-in-fact. The common thread is the theory that Plaintiffs, as Government employees, provided various forms of information to Treasury and OPM, and that Defendants' actions in allowing certain members of the Government to access agency records compromises or could compromise an expectation of privacy in a way that injures them. But Plaintiffs fail to allege any public disclosure of any information accessed by DOGE-affiliated personnel, let alone any public disclosure of Plaintiffs' information. That is a crucial distinction for purposes of Article III standing.

As an initial matter, Plaintiffs have not alleged any analogous harm in the common law or a harm traditionally recognized by courts. At most Plaintiffs claim "privacy rights afforded to federal employees as well as . . . American citizens in general" and that there has been a "unlawful and flagrant intrusion into federal employee's privacy[.]" Compl. ¶¶ 4, 48. But this vague assertion made in passing does not illustrate any traditionally recognized harm. Plaintiffs' failure to plead such an analog is fatal to their standing—"plaintiffs proceeding under a statutory cause of action can establish a cognizable injury by 'identif[ying] a close historical or common-law analogue for their asserted injury' for which courts have 'traditionally' provided a remedy." *Garey v. James S. Farrin, P.C.,* 35 F.4th 917, 921 (4th Cir. 2022) (alteration in the original) (quoting *TransUnion*, 594 U.S. at 424); *see also O'Leary v. TrustedID, Inc*., 60 F.4th 240, 245 (4th Cir. 2023) (since plaintiff has not pleaded a nonspeculative connection "between the alleged statutory violation and identity theft," plaintiff's reliance on some abstract privacy interest in his SSN itself "bears no close relationship to a traditional or common-law analog.").

To be sure, even if they had identified some common law analog, such a proxy for harm would still be insufficient as applied here. First, the tort of intrusion upon seclusion is a poor fit for challenges to agency access-to-data decisions, as a majority of a three-judge panel of the Fourth Circuit recently concluded in granting the government's motion to stay a preliminary injunction against Treasury and other agencies in *American Federation of Teachers v. Bessent*, another challenge to DOGE affiliates' access to agency record systems. *See* No. 25-1282, 2025 WL

1023638 (4th Cir. Apr. 7, 2025.[2][3] As Judge Agee explained in his concurring opinion, joined by Judge Richardson, "[a]t its core, the harm contemplated by the common-law tort of intrusion upon seclusion includes an intrusion into an individual's private space." *Id.* at *2. And as Judge Agee correctly noted, other circuit decisions have "also concluded that the harm visited upon an individual by [the] intrusion upon seclusion must include some [] interjection into the private sphere." *Id*.

Indeed, in *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458 (7th Cir. 2020) (Barrett, J.)—which the Supreme Court cited in *TransUnion*—the court addressed the receipt of unwanted text messages sent to the plaintiffs' personal cell phones—i.e., actual intrusion into the peace and tranquility of the plaintiffs' use of their personal property. *Gadelhak*, 950 F.3d at 462. The same is true of *Dickson v. Direct Energy, LP*, 69 F.4th 338 (6th Cir. 2023), where the court found that "invasion-of-privacy-like harm[] flow[s] from unwanted telephonic communications" in part because such communications "interject[] [the caller] into [the recipient's] private sphere." *Id.* at 346. In *Lupia v. Medicredit, Inc.*, 8 F.4th 1184 (10th Cir. 2021), the court also found standing

---

[2] At the request of Judge King, the full Fourth Circuit considered the panel's decision for initial rehearing *en banc* and voted 8-7 to deny the request.

[3] Defendants acknowledge that two other courts in this District have concluded that the plaintiffs have standing to pursue their Privacy Act claims in similar (though not identical) circumstances. *See Am. Fed'n of Labor & Congress of Indus. Orgs. v. Dep't of Labor*, --- F. Supp. 3d ----, 2025 WL 1129227, at *8 (D.D.C. Apr. 16, 2025); *All. for Retired Americans v. Bessent*, --- F. Supp. 3d ---, 2025 WL 740401, at *14-17 (D.D.C. Mar. 7, 2025). In addition, another Fourth Circuit en banc decision addressing alleged violations of the Privacy Act by the Social Security Administration found on a preliminary basis that Plaintiffs have standing. *See Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. Soc. Sec. Admin. ("AFSCME")*, No. 25-1411, 2025 WL 1249608 (4th Cir. Apr. 30, 2025). Defendants respectfully disagree with those decisions for the reasons stated herein. In *AFSCME*, moreover, the government filed an application to the United States Supreme Court on April 30 for a stay of the district court's preliminary injunction pending consideration of the government's appeal to the Fourth Circuit, and if the Fourth Circuit affirms the injunction, pending the timely filing and disposition of a petition for a writ of certiorari and any further proceedings in the Supreme Court. *See Soc. Sec. Admin., et al.., Applicants v. Am. Fed'n of State, Cnty. & Mun. Emps., et al.*, 24A1063. The government's application to the Supreme Court is fully briefed

based on unwanted telephone communications because they were an "unwanted intrusion into [the] plaintiff's peace and quiet." *Id.* at 1192. And in *Six v. IQ Data Int'l, Inc.*, 129 F.4th 630 (9th Cir. 2025), the court explained that other decisions have "found that the harm caused by unwanted communications bears a close relationship to intrusion upon seclusion." *Id.* at 634.

In *American Federation of Teachers*, Judge Agee found that alleged accessing of personal information in government record systems by DOGE team members within agencies does not allege "any interjection into the private sphere analogous to . . . unsolicited mailings . . . or unsolicited phone calls" and accordingly rejected analogizing such access to the common law tort of intrusion upon seclusion. *AFT*, 2025 WL 1023638, at *2*; see also id*. at *4-5 (Judge Richardson's concurring opinion) (agreeing that plaintiffs lacked standing and rejecting analogy to intrusion upon seclusion).

At any rate, even if Plaintiffs could plausibly point to some common law analog injury, Plaintiffs' purported harms are not cognizable. Plaintiffs allege that "Defendants' actions resulted in . . . the disclosure of Plaintiffs and Class Members' records without prior written consent" in violation of the Privacy Act. Compl. ¶ 77. Defendants dispute Plaintiffs' claims that there was any impermissible disclosure. But even assuming—solely for purposes of the injury-in-fact analysis, *see, e.g.*, *Warth*, 422 U.S. at 502—that there had been such access, unauthorized access alone would not give rise to an actual concrete harm. The Supreme Court's decision in *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), leaves no doubt that a statutory violation is not, by itself, a cognizable Article III injury. *Id.* at 426-27.

Rather, "[o]nly those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that . . . defendant over that violation in federal court." *Id.* at 427 (emphasis in original). For Plaintiffs to establish some concrete harm, they would need to show not just *access* to their information, but that the information had been disclosed in a way that causes them harm, such as a public disclosure. *See TransUnion*, 594 U.S. at 434 n. 6 ("Many American courts did not traditionally recognize intra-company disclosures as actionable publications for

purposes of the tort of defamation.") (citations omitted); *see also Taylor v. Fed. Aviation Admin.*, 351 F. Supp. 3d 97, 104 (D.D.C. 2018) ("Thus, the wrongful possession of Plaintiff's personal information, without more, does not establish injury in fact."); *see also Hunstein v. Preferred Coll. & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240, 1245-50 (11th Cir. 2022) (en banc) (no cognizable injury from the disclosure of private information where plaintiff's information was sent from hospital to collection agency because disclosure was not public.). In *TransUnion*, individuals who had a credit report that classified them as terrorists disseminated to third-party businesses were deemed to have Article III standing because they "suffered a harm with a 'close relationship' to the harm associated with the tort of defamation." 594 U.S. at 432-33. Another example would be a data breach that caused real harm. *Compare In re OPM Data Sec. Breach Litig.*, 928 F. Supp. 3d 42, 55-58 (D.C. Cir. 2019) (per curiam) (finding that "hackers" accessed confidential information as part of a cyberattack and plaintiffs indicated subsequent misuse of that information), *with Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3d Cir. 2011) (finding that plaintiffs "alleged no misuse, and therefore, no injury" because all that is known was that a firewall was penetrated.), *and Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017) (same).

At bottom, Plaintiffs have alleged no public disclosure of any information accessed by DOGE-affiliated personnel—much less that Plaintiffs' specific and unique personal information has been viewed out of the "approximately 2 million federal employees." Compl. ¶ 26. Plaintiffs' far-fetched assumption that DOGE had accessed their individual PSI would be akin to finding a needle in a haystack. *See Am. Fed'n of Tchrs. v. Bessent*, No. 25-1282, 2025 WL 1023638, at *11 (4th Cir. Apr. 7, 2025) (Richardson, J., concurring) (questioning whether plaintiffs' information stored in government databases could be a part of intrusion upon seclusion at all because their information "is one row in various databases that are millions upon millions of rows long."); *see also In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F.3d 14, 29 (D.D.C. 2014) (finding that "until Plaintiffs can aver that their records have been viewed (or certainly will be viewed) [by a nefarious third-party], any harm to their privacy remains

speculative); *Barclift v. Keystone Cred. Servs., LLC*, 585 F.3d 748, 758-59 (E.D. Pa. 2022) ("Even assuming that the employees of the mailing vendor read Barclift's personal information, sharing her personal information with 'a small group of persons is not publicity.'" (citation omitted)), *aff'd*, 93 F.4th 136, 146 (3d Cir. 2024) ("Like our sister circuits, we conclude that the harm from disclosures that remain functionally internal are not closely related to those stemming from public ones.").

Nor does the cost of preventing some form of conjectural future harm create standing. Plaintiffs allege pecuniary harm based on their alleged purchase of varying forms of identity theft prevention plans. Compl. ¶¶ 19-23, 53(c), 53(f). Yet Plaintiffs cannot manufacture standing by "inflicting harm on themselves" to defend against an otherwise speculative injury. *In re Sci. Applications Int'l Corp*, 45 F.3d at 26; *see, e.g., Reilly*, 664 F.3d at 46 ("Appellants' alleged time and money expenditures to monitor their financial information do not establish standing" because costs incurred to check on a "speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims."); *Randolph v. ING Life Insurance & Annuity Co*., 486 F. Supp. 2d 1, 8 (D.D.C. 2007) (the "argument that the time and money spent monitoring a plaintiff's credit suffices to establish an injury overlook[s] the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized.") (internal quotation marks omitted).

In contrast, the purchase of identity theft protection services would constitute pecuniary harm if bought as a rational response to fraudulent acts stemming from the breach. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig*., 928 F.3d at 65-66 (finding "actual damages" when plaintiffs purchasing credit protection services had experienced fraudulent tax returns filed in their name, fraudulent loans taken out in their name, and fraudulent credit card accounts opened.). Consequently, Plaintiffs' costs of acquiring identity theft protection services for a harm that has not occurred, and is not likely to occur because there has been no public disclosure, does not

qualify as "actual damages" under *Cooper*. Finally, Plaintiffs claim that the alleged breach has caused anxiety and emotional distress. Compl. ¶¶ 4, 53. But "general anxiety does not establish standing." *Welborn v. Internal Revenue Serv.*, 218 F.Supp.3d 64, 77 (D.D.C. 2016).

2. Plaintiffs' Alleged Harms Are Speculative And Not Actual Or Imminent

To establish Article III standing, Plaintiffs must show that they have suffered injury-in-fact—"actual or imminent, not speculative" harm, "meaning that the injury must have already occurred or be likely to occur soon." *FDA v. Alliance for Hippocratic Med.*, 602 U.S. 367, 381 (2024). For an injury to be imminent, it must be "certainly impending"; mere "allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (cleaned up). In other words, injury cannot be established through "a 'highly attenuated chain of possibilities' predicated on 'guesswork as to how independent decisionmakers will exercise their judgment.'" *Indus. Energy Consumers of Am. v. FERC*, 125 F.4th 1156, 1163 (D.C. Cir. 2025) (quoting *Clapper*, 568 U.S. at 410).

Plaintiffs' complaint raises concerns about how those working for USDS might use information after they access it, but these allegations rely on precisely the "highly attenuated chain of possibilities," warned of in *Clapper*, 568 U.S. at 410, involving at least the following links: (1) Defendants give employees access to particular systems of records; (2) those employees actually access those systems; (3) the employees then find and access Plaintiffs' unique PSI to attain the sort of confidential information within those systems that give rise to Plaintiffs concerns; (4) the employees improperly use that information in a way that harms Plaintiffs, such as by leaking their PSI to the public or a criminal actor; and (5) Plaintiffs suffer pecuniary harm as a result of the use of the information.

Plaintiffs speculate that such a use of confidential information is possible because "[Elon] Musk's people could easily find individuals in databases or clone entire servers and transfer that secure information somewhere else" and that data "could be [Musk's] forever[.]" Compl. ¶ 42. But "the mere existence, without more, of a governmental investigative and data-gathering activity

that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose," is not enough for standing purposes. *Laird v. Tatum*, 408 U.S. 5, 10-11 (1972); *see also Murthy v. Missouri*, 603 U.S. 43, 57 (2024) (finding no standing where a theory of injury "relies on a highly attenuated chain of possibilities"); *see also Welborn*, 218 F.Supp.3d at 77 (finding no standing where the likelihood that plaintiff will suffer further harms remains "entirely speculative and depends on the decisions and actions of one or more independent, and unidentified, actor(s).").

Plaintiffs also maintain that the alleged breach makes them "vulnerable to fraud, cyber-attack, and actual theft." Compl. ¶¶ 4, 51. This too misses the mark. Plaintiffs do not have standing based on risk alone. *See Clapper*, 133 S. Ct. at 1150 (expressing "our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."); *Randolph v. ING Life Insurance & Annuity Co*., 486 F.2d 1, 7-8 (D.D.C. 2007) (finding that it was "mere speculation" to assume "that at some unspecified point in the indefinite future they w[ould] be the victims of identity theft."); *Whitaker v. Health Net of Cal., Inc.,* No. 11-910, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012) ("[P]laintiffs do not explain how the loss here has actually harmed them . . . or that third parties have accessed their data.").

Any hypothesized harm stemming from USDS access to agency systems is precisely the type of conjectural and hypothetical harm that is insufficient to allege standing. *See, e.g.*, *Doe v. OPM*, No. 25 Civ. 234 (RDM), 2025 WL 513268, at *6 (D.D.C. Feb. 17, 2025) ("Plaintiffs must do more than point to a decade-old failure to protect sensitive data; they must show that OPM computer systems [accessed by new OPM employees] are at imminent risk of cyberattack and that this risk would be mitigated were the agency required" to implement measures mandated by the Privacy Act); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) ("Plaintiffs lack standing" where backup data tapes were stolen and most plaintiffs alleged only a risk of harm "because their claims are future-oriented, hypothetical, and conjectural."); *Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9,

2010) ("Plaintiff's alleged injury of an increased risk of identity theft is far too speculative."); *Amburgy v. Express Scripts, Inc.*, 671 F.2d 1046, 1052 (E.D. Mo. 2009) (no standing where "plaintiff does not claim that his personal information has in fact been stolen and/or his identity compromised" in the data breach).

A recent opinion analyzing similar allegations related to USDS access found that harms alleging "risk" of "identity theft," and a "risk" of "further dissemination of their data" are all entirely conjectural. *Univ. of California Student Ass'n v. Carter*, No. CV 25-354 (RDM), 2025 WL 542586 at *6 (D.D.C. Feb. 17, 2025) (stating that plaintiffs provided no evidence, "beyond sheer speculation, that would allow the Court to infer that [] DOGE staffers will misuse or further disseminate this information."); *see also Am. Federation of State, Cnty. & Mun. Emps*., *AFL-CIO v. Soc. Sec. Admin*., No. CV ELH-25-0596, 2025 WL 868953 at *34-35 (D. Md. Mar. 20, 2025) (finding that plaintiffs' concerns of possible identity theft arising from the "unfettered access to [PSI] provided by SSA to the DOGE Team, is insufficient to establish standing."); *see also Beck v. McDonald*, 848 F.3d 262, 274-75 (4th Cir. 2017) (the "mere theft" of personal information, "without more, cannot confer Article III standing."). So too here. Plaintiffs do not possess standing because they fail to assert anything more than speculation, conjecture, and attenuated theories of harm.

3. Plaintiffs' Alleged Harms Vis A Vis Their Family Members Are Not Particularized

Injury-in-fact should also be "particularized" to the plaintiff and not a "generalized grievance." *Alliance*, 602 U.S. at 381. And "[w]hen the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult' to establish." *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 489 (4th Cir. 2025) (quoting *Summers v. Earth Island Inst*., 555 U.S. 488, 493-94 (2009)).

Plaintiffs' claim that they are harmed because they cannot avoid having "PSI for themselves and their family members maintained in government records . . . " and that they have suffered or are at risk of suffering the compromise of their family member's PSI. Compl. ¶¶ 49,

53(b) 53(e). But Plaintiffs cannot claim their family member's harm as their own for purposes of standing. The injury-in-fact test requires that "the party seeking review be himself among the injured." *Sierra Club v. Morton*, 405 U.S. 727, 734-35 (1972). Plaintiffs' alleged harms vis a vis their family members likewise fail to confer standing.

II. Plaintiffs' Privacy Act Claim Should Be Dismissed

As the Supreme Court has said "on many occasions . . . a waiver of sovereign immunity must be 'unequivocally expressed' in statutory text." *F.A.A. v. Cooper*, 566 U.S. 284, 290 (2012). "Any ambiguities in the statutory language are to be construed in favor of immunity, so that the Government's consent to be sued is never enlarged beyond what a fair reading of the text requires." *Id.* (citations omitted). The question is not "whether Congress has consented to be sued for damages" in the abstract, but the "*scope* of that waiver," such that courts "construe any ambiguities in the scope of a waiver in favor of the sovereign." *Id.* at 291 (emphasis in original).

Plaintiffs' Privacy Act claim should be dismissed because the relief they seek goes beyond the statute's waiver of sovereign immunity. As discussed below, although Plaintiffs seek monetary damages and injunctive relief, Plaintiffs do not allege any actual damages resulting from the alleged Privacy Act violation, and the injunctive relief they seek is not authorized under the Privacy Act.

A. Plaintiffs Have Not Adequately Alleged Any "Actual Damages"

To properly state a claim for damages under the Privacy Act, Plaintiffs must plead "actual—that is, pecuniary or material—harm." *Cooper*, 566 U.S. at 296. In *Cooper*, the Supreme Court held that the term "actual damages" in the statute is "limited to proven pecuniary or economic harm," which is a form of "special damages" that must be "specially pleaded and proved." 566 U.S. at 295, 299.

The United States retains sovereign immunity under the Privacy Act for all non-economic harms, including "loss of reputation, shame, mortification, injury to the feelings and the like." *Id.* at 295-96, 299, 304, and failure to establish "actual damages" is fatal to monetary recovery. *Id.* at

295 (explaining that "the Privacy Act's remedial provision authorizes plaintiffs to recover . . . but only if they prove at least some 'actual damages'") (quoting 5 U.S.C. § 552a(g)(4)(A)). Claims for damages based on emotional harm are not allowed. *Id.* at 304 ("[T]he Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress. Accordingly, the Act does not waive the Federal Government's sovereign immunity from liability for such harms."); *Welborn*, 218 F.3d at 82 (finding that "[t]he Privacy Act does not allow a claim for damages based on . . . emotional harm," and "[a]s a result, Plaintiff[ ] must specifically allege actual damages to survive a motion to dismiss for failure to state a claim.). Further, the Court "should not assume actual damages based on a conclusory statement that Plaintiffs . . . 'have suffered or are at increased risk of suffering from' a list of potential harms." *Welborn*, 218 F.3d at 82-83. Accordingly, Plaintiffs must plead actual damages under the strictures of the Privacy Act to survive a motion to dismiss for failure to state a claim.

Applying these principles, courts in this District have routinely dismissed Privacy Act claims where concrete allegations of calculable pecuniary loss are absent. *See, e.g.*, *Stewart v. Kendall*, 578 F. Supp. 3d 18, 23-24 (D.D.C. 2022) (dismissing claim because the plaintiff failed to plausibly allege pecuniary damages caused by the alleged violation); *Bozgoz v. James*, No. 19-0239 (ABJ), 2020 WL 4732085, *11-12 (D.D.C. Aug. 14, 2020) (dismissing claim because plaintiffs alleged only general damages and "d[id] not specify any pecuniary losses they incurred"); *compare Welborn*, 218 F.3d at 82 (dismissing claims based on alleged reputational and emotional harm and other conclusory allegations, because plaintiffs failed to "detail[] actual pecuniary or material damage" in their complaint); *with In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 65-66 (D.C. Cir. 2019) (concluding plaintiffs had alleged "actual damages" after purchasing credit protection and/or credit repair services following a data breach, and had fraudulent accounts established and false tax returns filed in their names).

Here, Plaintiffs allege that they will be harmed through (1) the loss of opportunity to control how their data is used; (2) the compromise of their family members and their own PSI; (3) costs

associated with prevention, detection, and recovery from identity theft and/or unauthorized use of various accounts; (4) lost opportunity cost from expended efforts and loss of productivity from attempting to mitigate any consequences from the alleged breach; (5) continued risk to their PSI and that of their family members; and (6) current and future costs associated with monitoring, preventing, detecting, contesting, and repairing the impact of the allegedly compromised PSI data. Compl. ¶¶ 19-23.

Yet, Plaintiffs fail to plead facts showing that they have sustained *any* calculable monetary loss as a result of the Defendants' alleged conduct. Plaintiffs state that they have suffered "damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress." Compl. ¶ 53. But *Cooper* expressly instructs there is no waiver of sovereign immunity under the Privacy Act for damages relating to mental or emotional distress. *See* 566 U.S. at 287, 295-96. And otherwise, the conclusory allegations submitted by Plaintiffs are insufficient. *Cooper*, 566 U.S. at 295; *see also Welborn*, 218 F.3d at 82 (declining to assume actual damages based on conclusory statements in the plaintiffs' complaint). Accordingly, Plaintiffs fail to allege actual damages under the Privacy Act.

Moreover, of these various alleged harms, only the purported costs associated with identity theft mitigation could even plausibly be construed as actual pecuniary or material damage. But even those mitigation costs are insufficient to be considered "actual damages" because there is no "substantial risk of future harm" to be mitigated. *Stewart v. Kendall*, 578 F. Supp. 3d 18, 24 (D.D.C. 2022) (finding that "mitigation costs incurred to prevent future injury can qualify as actual damages and satisfy the injury-in-fact requirement only if there is at least a substantial risk of future harm."); *see also* Clapper, 568 U.S. at 414. As discussed above, it is purely speculative whether the alleged access provided to DOGE team members within agencies will result in any theft of Plaintiffs' identity. Plaintiffs' hypothetical harm of having "no assurance that their PSI will receive the protection that federal law affords" along with other hypothesized future harms does not suffice. Compl. ¶¶ 19-23. A "vague description of the harms allegedly sustained as a

result of [an agency's] disclosure cannot support a demand for actual damages that must be 'limited to proven pecuniary or economic harm.'" *Glass v. U.S. Dep't of Justice*, 279 F.3d 279 (D.D.C. 2017) (quoting *FAA v. Cooper*, 566 U.S. 284, 299 (2012) (emphasis omitted)).

This is unlike the case of *Attias* where the Court found that plaintiffs plausibly alleged a substantial risk of identity theft because the breach "exposed [their] social security and credit card numbers to an intruder." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627-28 (D.C. Cir. 2017). And Plaintiffs claims are further in contrast to *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d at 58-59, where there was an actual data breach that exposed plaintiffs' social security numbers, fingerprints, and other private information to third parties. It was on that basis the court found that mitigation costs for a substantial risk of future harm were warranted. *Id*.

Plaintiffs have also not credibly plead that their particular, personal information was unlawfully accessed, disclosed, or stolen. Plaintiffs alleged that they learned "about Defendants' breaches of [their] PSI from media reports," but they do not cite those media reports nor explain how they were particularized to them. Compl. ¶¶ 19-23. Plaintiffs seemingly theorize that because OPM and Treasury store Plaintiffs' PSI, that DOGE's access to such information necessarily included their unique personal information. *Id.* ¶¶ 34, 36, 38, 42, 45-53.

These naked allegations, without more, do not suffice to connect their alleged pecuniary harm to the challenged conduct. Plaintiffs do not allege—much less establish—that USDS affiliated persons have disclosed their own personal information publicly, or that USDS itself has accessed Plaintiffs' information, let alone in any way that causes concrete harm. Unsupported legal conclusions, such as Plaintiffs' claims of an alleged breach of their unique PSI, are not to be implicitly assumed as true on its face. *See Food & Water Watch*, 808 F.3d at 913 (noting that we need not "assume the truth of legal conclusions [or] accept inferences that are unsupported by the facts set out in the complaint" (quoting *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015))). The Complaint only alleges that Plaintiffs learned through media reports that their PSI had been breached. Compl. ¶¶ 19-23. And that Defendant Scales was allowed to access a "massive database

holding information on millions of federal employees, including Plaintiffs' PSI." *Id*. at ¶ 36. But Plaintiffs cannot sufficiently claim that their purchase of identity theft detection services is tied to any specific disclosure of their information.

Put another way, Plaintiffs must allege "actual damages" *connected to* the adverse effect to "qualify" under the Act. *Doe v. Chao,* 540 U.S. 614, 620-27 (2004); *Mandel v. U.S. Office of Pers. Mgmt.,* 244 F. Supp. 2d 146, 153 (E.D.N.Y. 2003) (holding that plaintiff must establish a "causal connection" between agency violation and adverse effect). Thus, Plaintiffs "must establish not only that [they were] 'adversely affected' by the improper disclosure, *but also* that [they] suffered 'some harm for which damages can reasonably be assessed.'" *Mulhern v. Gates,* 525 F. Supp. 2d 174, 181-82 (D.D.C. 2007) (quoting *Doe v. Chao,* 540 U.S. at 621). Plaintiffs fail to make such a credible connection here.

It is speculative at best to assume that any members of USDS had read Plaintiffs' individual data. *Reilly,* 664 F.3d at 40 (finding that it would be speculative to assume that the alleged data thief had "read, copied, or understood the data."); *see Philippeaux v. United States*, No. 10 CIV. 6143 NRB, 2011 WL 4472064 at *9 (S.D.N.Y. Sept. 27, 2011) ("[P]laintiff does not 'know[] with absolute certainty whether or not any pertinent records have been removed" and as a result his assertions were not sufficient to state a claim under the Privacy Act because he could not "adequately show that he was adversely affected by any disclosure."). *See, e.g.*, *Wrocklage v. DHS*, 769 F.3d 1363, 1369 (Fed. Cir. 2014) (disclosure under the Privacy Act "require[es] not just transmission, but actual viewing or imminent viewing by another"); *Luster v. Vilsack*, 667 F.3d 1089, 1098 (10th Cir. 2011) (possibility that record might be revealed does not constitute "disclosure" under the Privacy Act); *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d 14, 28-29; 5 C.F.R. § 297.102 ("Disclosure means providing *personal review* of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian." (emphasis added)); *but see* OMB Guidelines, 40 Fed. Reg. 28948, 28953 (July 9,

1975) ("A disclosure may be either the transfer of a record or the granting of access to a record."). Thus, for the aforementioned reasons, Plaintiffs fail to state a claim.

B. Plaintiffs Are Not Entitled to the Other Forms of Relief They Seek

Plaintiffs request "injunctive relief." Compl. ¶ 2. But the Privacy Act allows for injunctive relief in only two narrow circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C. § 552a(g)(1)(A), (g)(2)(A); and (2) to order an agency to allow an individual access to his records. *Id*. § 552a(g)(1)(B), (g)(3)(A). Yet Plaintiffs do not request injunctive relief under either circumstance. Injunctive relief, as the D.C. Circuit has recognized, is not available for any other situation arising out of the Privacy Act. *See*, *e.g.*, *Sussman v. U.S. Marshal Serv*., 494 F.3d 1106, 1122 (D.C. Cir. 2007) ("We have held that only monetary damages, not declaratory or injunctive relief, are available to § 552a(g)(1)(D) plaintiffs . . . .") (citing *Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988)); *Doe v. Chao*, 435 F.3d 492, 504 (4th Cir. 2006) ("[S]ubsection (g)(1)(D) of the Privacy Act does not allow courts to grant injunctive or declaratory relief.") (collecting cases).

Plaintiffs also request equitable and declaratory relief. These forms of relief are often folded into the broad scope of injunctive relief, but for the avoidance of doubt, both equitable and declaratory relief are also proscribed under the Act. *See Hastings v. Judicial Conference*, 770 F.2d 1093, 1104 (D.C. Cir. 1985) (concluding that equitable relief is not available under the Privacy Act because "such relief [is] not . . . among those expressly made available to remedy past disclosures"); *see also Radack v. U.S. Dep't of Just*., 402 F.2d 99, 104 (D.D.C. 2005) ("[T]he Privacy Act provides only for monetary relief when an agency makes illegal disclosures."). Accordingly, Plaintiffs are not entitled to injunctive, equitable, or declaratory relief.

III. The Privacy Act Does Not Allow Suit Against Individually Named Defendants

Plaintiffs filed suit against Treasury Secretary Scott Bessent, Charles Ezell, Amanda Scales, Brian Bjelde, and Gregory Barbaccia in their official capacities. However, the Privacy Act does not provide for a civil action against individuals. *See Martinez v. Bureau of Prisons*, 444

F.3d 620, 624 (D.C. Cir. 2006) (finding that the district court properly dismissed the named individual defendants "because no cause of action exists that would entitle appellant relief from them under the Privacy Act[.]"); *see also Abdelfattah v. U.S. Dep't of Homeland Sec*., 787 F.3d 524, 533 n. 4 (D.C. Cir. 2015) ("[T]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individual officials.") (citations omitted); *see also Afifi v. Lynch*, 101 F. Supp. 3d 90, 104 n.8 (D.D.C. 2015) ("[P]laintiff may not bring suit under the Privacy Act against the official capacity defendants and must instead bring suit against the appropriate agency."). The Act only authorizes a civil action against an "agency." 5 U.S.C. § 552a(g)(1). Moreover, because claims against individuals in their official capacity are effectively claims against the agency, Plaintiffs would not be prejudiced if their claims against individual Defendants were dismissed. Hence Plaintiffs' claims against the individually named Defendants should be dismissed.

IV. Plaintiffs Are Not Entitled To A Jury Trial

Plaintiffs also demand a jury trial. Compl. at 23. This too is not permitted. In general, the United States is immune from being sued unless it consents. *United States v. Sherwood*, 312 U.S. 584, 586 (1941); *United States v. Testan*, 424 U.S. 392, 399 (1976). Even when the Sovereign does consents, the Seventh Amendment does not grant a plaintiff a right to a jury trial in actions against the United States. *Lehman v. Nakshian*, 453 U.S. 156, 160-161 (1981) ("It has long been settled that the Seventh Amendment right to trial by jury does not apply in actions against the Federal Government."). Thus, when the government does consent to being sued, the plaintiff has a right to a jury trial only when the right has been "unequivocally expressed" by Congress. *Id*. The Privacy Act is silent as to any right to a jury trial. *See* 5 U.S.C. §§ 552; 522a. Therefore Plaintiffs have no right to a jury trial. *See Buckles v. Indian Health Serv./Belcourt Serv. Unit*, 268 F. Supp. 2d 1101, 1102-03 (D.N.D. 2003) (holding that the Privacy Act does not provide plaintiff with the right to a jury trial.).

V. The Court Should Resolve The Threshold Questions Of Standing And Failure To State A Claim Before This Matter Proceeds Any Further

Plaintiffs seeks class certification for "[a]ll current, former, and prospective employees of the United States whose [PSI] was accessed without their prior written authorization from OPM and Department of Treasury beginning in January 2025." Compl. ¶ 55.

Rather than undertaking class certification or any other proceedings, the Court should rule on the issues raised in the Government's motion to dismiss. It is unnecessary to undertake class certification prior to resolving this issue. Rule 23 of the Federal Rules of Civil Procedure states that "[a]t an early practicable time after a person sues as a class representative, the court must determine by order whether to certify the action as a class action." Fed. R. Civ. P. 23(c)(1)(A). This "early practicable time" formulation "does not indicate whether it should be made before or after dispositive motions." William Rubenstein *et al.*, Newberg on Class Actions § 7:9 (5th ed. 2020). That treatise furthermore notes that "courts have been willing to rule on motions for summary judgment prior to class certification in circumstances in which it would facilitate efficient resolution of the case." *Id.* § 7:10 (citing cases).

Consistent with this, courts in the jurisdiction have stayed class certification pending resolution of the motion to dismiss. *See Kang v. Dep't of Homeland Sec.*, No. CV 21-2944 (RJL), 2022 WL 4446385, at *2 (D.D.C. Sept. 23, 2022); *see also Fischer v. D.C.*, No. 24-CV-00044 (CRC), 2025 WL 894445, at *3 (D.D.C. Mar. 24, 2025); *see also Howard v. Gutierrez*, 474 F.2d 41, 44 (D.D.C. 2007). Similarly here, the Court should resolve Defendants' Motion to Dismiss before class certification as the Motion may be dispositive to the litigation.

CONCLUSION

For the foregoing reasons, the Court should grant Defendants' Motion to Dismiss Plaintiffs' Complaint.

Dated: May 19, 2025

Respectfully submitted,

YAAKOV M. ROTH
Acting Assistant Attorney General

MARCIA BERMAN
Assistant Director, Federal Programs Branch

/s/ Pierce J. Anon
PIERCE J. ANON (N.Y. Bar # 6184303)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 305-7573
Email: pierce.anon@usdoj.gov

Counsel for Defendants