

**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. 25-cv-407 (CRC)

MEMORANDUM OPINION AND ORDER

Upon taking office for his second term, President Trump created the Department of Governmental Efficiency (“DOGE”) with the goal of “improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems.” Exec. Order No. 14,158, 90 Fed. Reg. 8441, § 4 (Jan. 20, 2025). DOGE immediately staffed up with young computer engineers—many of whom had worked for companies associated with Elon Musk and had little or no prior government experience—and then sought access to agency databases across the federal government. Some of the targeted systems housed Americans’ most sensitive personal information, from Social Security and passport numbers to tax and payroll records. Widespread litigation ensued, with concerned citizens and organizations representing them suing to enjoin DOGE and its staffers from securing (or maintaining) access to their confidential records.

This putative class action also stems from DOGE’s access to government data. But rather than request injunctive relief, Plaintiffs, five current government employees, seek damages. On behalf of themselves and similarly situated federal workers, they allege that the Office of Personnel Management (“OPM”) and Department of the Treasury (together,

“Defendants” or “agencies”) violated the Privacy Act (“the Act”) by giving DOGE access to internal systems containing their sensitive information. Defendants have moved to dismiss Plaintiffs’ complaint on two grounds. First, they contend that Plaintiffs lack standing because the alleged disclosure of their data to DOGE does not constitute an Article III injury-in-fact. Second, they assert that Plaintiffs have not alleged that they suffered actual damages, as required under the Privacy Act.

The Court will deny Defendants’ motion and allow the case to proceed to discovery. Like other courts in this district that have considered the issue, the Court finds that the alleged provision of Plaintiffs’ sensitive, individualized data to DOGE under the circumstances described in the complaint is akin to the common-law harm of intrusion upon seclusion, which the Supreme Court has indicated is a sufficiently “concrete” Article III injury. See TransUnion LLC v. Ramirez, 594 U.S. 413, 425 (2021). Plaintiffs thus have standing to pursue their Privacy Act claim. As to that claim, while it may be relatively novel in the absence of a malicious infiltration of the systems in question, Plaintiffs have adequately alleged that they suffered actual damages by purchasing identity theft protection services to guard against potential fraud. That is so because those purchases appear reasonable given contemporaneous public reporting on DOGE’s access to their data and its possible mishandling of data elsewhere within the government. The reasonableness of that decision has only been confirmed by the government’s recent admission that DOGE staffers have in fact mishandled agency data in precisely the ways Plaintiffs feared.

I. Background

Unless otherwise noted, the Court draws the following background from Plaintiffs’ First Amended Class Action Complaint (“FAC”). Defendants no doubt dispute many of Plaintiffs’ allegations.

Plaintiffs Denise Nemeth-Greenleaf, Jason Judkins, Jon Michel, Donna Nemeth, and Michael Rifer are employed by five different federal agencies. FAC ¶¶ 2, 14–18. The Bureau of the Fiscal Service, which processes payments for the Department of Treasury, collects and maintains a variety of Plaintiffs’ (and other federal employees’) personal information, including their Social Security numbers and bank account information. Id. ¶ 20. OPM, which handles human resources for federal employees, also maintains a comprehensive trove of Plaintiffs’ data, including their birth certificates, documents reflecting their Social Security numbers and birth dates, health insurance information, disability status, and more. Id. ¶¶ 21–22.

On January 20, 2025, President Trump renamed the United States Digital Service as the United States DOGE Service (“DOGE”) and moved it within the Executive Office of the President. See Exec. Order 14,158, 90 Fed. Reg. 8441, § 3 (Jan. 20, 2025). DOGE immediately started seeking access to government databases. FAC ¶ 28. In late January, Treasury Secretary Scott Bessent granted DOGE-affiliated individuals “full access” to the Bureau of the Fiscal Service’s data and computer systems. Id. ¶ 29. According to Plaintiffs, these individuals had not obtained security clearances or completed the requisite training before gaining access to federal employees’ personal information. Id. For example, Plaintiffs claim that the Treasury Department gave 25-year-old Marko Elez, who was not yet a government employee, “direct access” to its payment systems. Id. ¶ 30. Citing media reports, Plaintiffs allege that Elez later sent an unencrypted spreadsheet with sensitive data to individuals outside of the department. Id.

Plaintiffs describe something similar at OPM, where the agency allegedly gave control over a sensitive personnel database to former Musk employee Amanda Scales, who Plaintiffs say was not yet employed by the government. Id. ¶ 31. Similarly inappropriate disclosures to other Musk associates followed, according to the complaint. Id. ¶¶ 32–34.

Experts immediately sounded public alarms about DOGE’s access to government data. They voiced concerns about changes in agency security protocols, warning that data could be transferred or siphoned elsewhere, potentially for private use. Id. ¶¶ 35–38. They also intoned that critical data was vulnerable to foreign adversaries and malevolent hackers. One expert opined, “If I were a nation like China, Russia, or Iran, I’d be having a field day with a bunch of college kids running around with sensitive federal government data on unencrypted hard drives.” Id. ¶ 48 (quoting Isaac Stanley-Becker, Greg Miller, Hannah Natanson & Joseph Menn, Musk’s DOGE Agents Access Sensitive Personnel Data, Alarming Security Officials, Wash. Post (Feb. 6, 2025), <https://perma.cc/GK7P-S7M5>).

In May 2025, National Labor Relations Board (“NLRB”) IT staffer Daniel Berulis, who oversaw the agency’s day-to-day cybersecurity operations, lodged a whistleblower disclosure with Congress (“Berulis Disclosure”). Id. ¶¶ 49, 52. Among other red flags, Berulis revealed that after DOGE gained access to the NLRB’s internal systems, there was a “spike in data leaving the agency,” and a Russian IP address repeatedly tried to access the systems. Id. ¶¶ 49–50. Berulis explained that he had been ordered not to follow standard operating procedures with regard to DOGE’s accounts or DOGE staffers’ access to information. Id. ¶ 52. Berulis also reported that DOGE representatives may not have followed proper security protocols for their accounts. Id. ¶¶ 55–56. And he ultimately discovered that data containing sensitive information

of parties with business before the agency had been transferred from the agency's systems to an unknown external location. Id. ¶ 63.

All the named Plaintiffs report purchasing identity theft protection services at some point following DOGE being given access to the computer systems and data in question. Id. ¶¶ 14–18. Moreover, Ms. Nemeth-Greenleaf claims to have identified fraudulent purchases in April 2025 on the debit card associated with the account where she receives her government salary. Id. ¶ 85. And Mr. Rifer reports learning from McAfee that his personal email address, which was on file with the government, was found on the “dark web” in May 2025. Id. ¶ 83.

Plaintiffs filed an initial class action complaint in February 2025. After Defendants moved to dismiss, the Court granted Plaintiffs leave to file the operative FAC. Defendants now move to dismiss that complaint for lack of subject matter jurisdiction and failure to state a claim. Plaintiffs oppose. The Court held a hearing on Defendants' motion on January 20, 2026.

II. Analysis

Defendants move to dismiss the complaint on two grounds. First, they contend that Plaintiffs lack standing because they have not alleged an injury-in-fact that is traceable to Defendants' actions. Second, they argue that Plaintiffs have failed to state a Privacy Act claim because they have not pled actual damages, which is a necessary element of a claim under the statute. The Court takes each argument in turn.

A. Standing

At the threshold, the government contends that Plaintiffs' standing is foreclosed by a June 2025 Supreme Court ruling that stayed pending appeal a district court's preliminary injunction limiting DOGE affiliates' access to records at the Social Security Administration (“SSA”). See

Defs.’ Reply at 3–5 (citing Soc. Sec. Admin. v. Am. Fed’n of State, Cnty., & Mun. Emps., 145 S. Ct. 1626 (2025) (“AFSCME”)).¹

A summary order by the Supreme Court on a temporary-stay application lacks the same precedential value as an opinion based on full briefing and oral argument. See Lunding v. N.Y. Tax Appeals Tribunal, 522 U.S. 287, 307 (1998). But when the Supreme Court speaks, however softly, this Court listens. See e.g., Harris County v. Kennedy, 786 F. Supp. 3d 194, 218 (D.D.C. 2025) (Cooper, J.) (finding that plaintiffs challenging HHS grant rescissions were unlikely to succeed on certain of their claim because the claims were foreclosed by the Supreme Court’s summary stay order in Department of Education v. California, 604 U.S. 650 (2025)). The Court follows “even probabilistic holdings” that provide “top-line conclusions,” recognizing both the importance of any determination, even an interim one, that the Supreme Court reaches and the precedential value of the reasoning underlying it. Nat’l Inst. Of Health v. Am. Pub. Health Ass’n, 145 S. Ct. 2658, 2663–65 (2025) (Gorsuch, J., concurring in part and dissenting in part).

But the Supreme Court did not offer even a probabilistic conclusion about standing in AFSCME. The Court’s stay order spanned only three paragraphs over a page and a half of text in the Supreme Court Reporter. The first paragraph summarized the relevant factual and procedural background. The second laid out the standards governing a stay pending appeal and a conclusory finding that those factors had been met. And the third described the particulars of the Court’s judgment. The entirety of the Court’s finding with respect to the applicable stay factors (in the second paragraph) reads as follows:

After review, we determine that the application of these [stay] factors in this case warrants granting the requested stay. We conclude that, under the present

¹ Because it goes to the Court’s jurisdiction, the Court will consider this argument even though it was squarely raised for the first time in Defendants’ reply brief.

circumstances, SSA may proceed to afford member of the SSA DOGE Team access to the agency records in question in order for those members to do their work.

AFSCME, 145 S. Ct. at 1626. Standing is not mentioned at all. Nor is it otherwise evident that a lack of standing led to the ruling.² To the contrary, given that the matter reached the Court on an application to stay preliminary relief, it appears more likely that the Court granted the application because it believed—as three other courts in this district did in similar cases—that the AFSCME plaintiffs did not face irreparable harm. Cf. Univ. of Cal. Student Ass’n v. Carter, 766 F. Supp. 3d 114, 120–23 (D.D.C. 2025) (denying a motion for TRO for lack of irreparable harm because, among other reasons, the Privacy Act makes damages available); Am. Fed’n of Lab. & Cong. of Indus. Orgs. v. Dep’t of Lab., No. 25-cv-339 (JDB), 2025 WL 1783899, at *13–15 (D.D.C. June 27, 2025) (same at preliminary injunction stage); All. for Retired Ams. v. Bessent, 770 F. Supp. 3d 79, 106–11 (D.D.C. 2025) (denying a motion for preliminary injunction for lack of irreparable harm but without mentioning damages).

This case also differs from AFSCME with respect to the relief sought. The AFSCME plaintiffs requested an injunction preventing SSA from sharing data with DOGE, which may have hindered DOGE in its ostensible goal of improving the efficiency of government IT systems. Balancing the equities, the Supreme Court may have acted out of a desire not to impede executive-branch operations while the litigation played out. The Court’s cursory explanation hints at such a motivation: “[U]nder the present circumstances, SSA may proceed to afford members of the SSA DOGE Team access to the agency records in question in order for those members to *do their work*.” AFSCME, 145 S. Ct. at 1626 (emphasis added). That

² Perhaps tellingly, the Fourth Circuit in American Federation of Teachers v. Bessent—a DOGE-data access challenge which the court described as “exceedingly similar” to AFSCME—held that plaintiffs likely lacked standing but did not apply AFSCME to its standing analysis. See 152 F.4th 162, 168, 171–74 (4th Cir. 2025).

concern, were it one for the Supreme Court, is not present here. Plaintiffs seek damages, which would not prevent the executive from pursuing its stated policy goals or operational choices during the pendency of the litigation. Accordingly, the AFSCME stay order does not foreclose Plaintiffs' standing in this case.

Turning to the meat of Defendants' standing challenge, the Court finds that Plaintiffs have pled an injury-in-fact.

Article III of the Constitution requires plaintiffs to demonstrate they possess standing; otherwise, there is no "case" or "controversy," and a court is powerless to consider the claims. See TransUnion, 594 U.S. at 423. To demonstrate standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." Id. (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)). At the motion to dismiss stage, plaintiffs must only "state a plausible claim" that they have standing. Humane Soc'y of the U.S. v. Vilsack, 797 F.3d 4, 8 (D.C. Cir. 2015).

To satisfy Article III's injury-in-fact requirement, a plaintiff's injury must be "real" and not "abstract." Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016). If a plaintiff pleads an intangible harm, a court must determine whether it has a sufficiently "'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." TransUnion, 594 U.S. at 424 (quoting Spokeo, 578 U.S. at 341). The injury need not be an "exact duplicate" of an established common-law harm, but there must be a "close historical or common-law analogue for [the] asserted injury." Id. Otherwise, the intangible harm is not sufficiently concrete to satisfy Article III. Id. Evidence of congressional intent "may be 'instructive'" in this analysis. Id. at 425 (quoting Spokeo, 578 U.S. at 341). The Supreme Court

has indicated that intrusion upon seclusion is a sufficiently “concrete” intangible harm upon which to base standing. See id.

The critical question, then, is whether Plaintiffs have offered allegations that are sufficiently similar to the common-law harm of intrusion upon seclusion. The traditional elements of the tort are (1) the intentional intrusion “upon the solitude or seclusion of another or his private affairs or concerns” and (2) that such intrusion “be highly offensive to a reasonable person.” All. for Retired Ams., 770 F. Supp. 3d at 102. The intrusion need not be physical. See Restatement (Second) of Torts § 652B (A.L.I. 1977).

Taking their allegations as true, Plaintiffs claim to have suffered an analogous injury. As to whether there was an intrusion upon the solitude of their private affairs and concerns, Plaintiffs trusted the government with their most sensitive data. And without their consent, the government allegedly shared it with yet to be employed, untrained, and unqualified individuals who did not have permission to access the data and who may have been motivated by private gain rather than public need. FAC ¶¶ 29–34. And the data in question is not just any information. It is foundational to Americans’ data-driven, internet-based lives. See, e.g., Wolf v. Regardie, 553 A.2d 1213, 1217–18 (D.C. 1989) (explaining that “examining a plaintiff’s private bank account” qualifies as one of the “types of invasion intrinsic in the tort of intrusion upon seclusion”). Knowledge of the information in Plaintiffs’ OPM and Treasury files would reveal the ins-and-outs of their professional and personal lives. Cf. All. for Retired Ams., 770 F. Supp. 3d at 103 (noting the “sensitivity of the information at issue”). Unauthorized perusal of this data is the digital equivalent of a stranger staring through a homeowner’s window to glean what she is doing or rifling through another’s papers to gather information about his private life. See Restatement (Second) of Torts § 652B (citing hypothetical examples of conduct that would

qualify as an intrusion upon seclusion). Plaintiffs have therefore adequately alleged the first element of the common-law harm.

As to the second element, there is little doubt that a reasonable person would find it offensive to allow an unauthorized person access to their most sensitive records. After all, there is a reason we do not go around sharing our bank account information and Social Security numbers with strangers: They are core to our digital security and privacy. See Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 710 (D.C. 2009) (“In this age of identity theft and other wrongful conduct through the unauthorized use of electronically-stored data, . . . conduct giving rise to unauthorized viewing of personal information such as a plaintiff’s Social Security number . . . can constitute an intrusion that is highly offensive to any reasonable person[.]”).

Any remaining doubt is settled by Congress’s passage of the Privacy Act. Congress may “elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.” Spokeo, 578 U.S. at 341 (alteration in original) (quoting Lujan, 504 U.S. at 578). The Privacy Act is intended to “protect the privacy of individuals identified in information systems maintained by Federal agencies.” Doe v. Chao, 540 U.S. 614, 618 (2004) (quoting Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896 (1974)). “Put simply, then, Congress ‘identified’ an individual’s interest in his information being viewed only by the federal agency that maintains it—and even then, only by those employees with a need to view it—as ‘a modern relative of a harm with long common law roots.’” Am. Fed’n of Lab. & Cong. of Indus. Orgs. v. Dep’t of Lab., 778 F. Supp. 3d 56, 72 (D.D.C. 2025) (quoting Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.)). The Privacy Act guaranteed individuals that the data they give over to the government would be protected—that they could feel “at peace” in a digital “sphere of seclusion.” Id. (citation omitted). Defendants

allegedly robbed Plaintiffs of that peace by disclosing the data to DOGE under the circumstances described in the complaint.

Citing Judge Agee’s concurrence in the Fourth Circuit’s grant of a stay pending appeal in American Federation of Teachers v. Bessent, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025), Defendants argue that intrusion upon seclusion requires more than merely looking at Plaintiffs’ data. Instead, Defendants claim that the agencies or DOGE must have disturbed Plaintiffs’ peace in a more tangible way, such as through an unwanted phone call or unsolicited text message. See Defs.’ Mot. at 9–10. However, Judge Agee’s analysis dealt with the District of Maryland’s application of Fourth Circuit precedents that do not apply here. See Am. Fed’n of Tchrs., 2025 WL 1023638, at *1–3.³ And Defendants’ more general argument—that there need have been a physical intrusion and direct contact with the victim—misunderstands intrusion upon seclusion’s historical roots. See Restatement (Second) of Torts § 652B (“[The invasion] may also be by the use of the defendant’s senses, with or without mechanical aids, to oversee or overhear the plaintiff’s private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.”).

Because the Court has determined that Plaintiffs’ injury-in-fact stems from an intangible harm analogous to the common-law harm of intrusion upon seclusion, Defendants’ traceability argument is irrelevant, as it focuses on other harms alleged in Plaintiffs’ complaint. See Defs.’ Mot. at 17–18 (analyzing whether the injury is traceable to Defendants’ actions “[e]ven if Plaintiffs can show an imminent risk of identity theft”). Taking Plaintiffs’ allegations as true,

³ In their reply, Defendants cite generally to the Fourth Circuit’s subsequent vacatur of the preliminary injunction. See Defs.’ Reply at 3. But this Court is not bound by that decision, any more than it is Judge Agee’s concurrence, and Defendants make no argument based on that case, other than to cite it.

Defendants caused an intrusion upon Plaintiffs' seclusion when they shared Plaintiffs' sensitive data under the circumstances described in the complaint. And the Court can redress Plaintiffs' alleged injuries through the remedies available in the Privacy Act.

B. The Privacy Act

The Court now turns to Defendants' arguments for dismissal of Plaintiffs' Privacy Act claim under Federal Rule of Civil Procedure 12(b)(6). A court deciding a Rule 12(b)(6) motion must "assume the truth of all material factual allegations in the complaint and 'construe the complaint liberally, granting plaintiff the benefit of all inferences that can be derived from the facts alleged.'" Am. Nat. Ins. Co. v. FDIC, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (quoting Thomas v. Principi, 394 F.3d 970, 972 (D.C. Cir. 2005)). To survive a 12(b)(6) motion, a complaint must contain sufficient factual matter, accepted as true, to state a plausible claim for relief. Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim is plausible if the pleaded facts allow the court to reasonably infer that the defendant is liable for the misconduct alleged. Iqbal, 556 U.S. at 678. While a court must take the complaint's factual allegations as true, it need not accept legal conclusions, and mere "labels" or "[t]hreadbare recitals of the elements of a cause of action . . . do not suffice." Id. (quoting Twombly, 550 U.S. at 555).

Under the Privacy Act, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency," unless "the individual to whom the record pertains" provides written consent or unless certain exceptions apply. 5 U.S.C. § 552a(b). When an agency fails to comply with the statute in such a way as "to have an adverse effect on an individual," the individual may sue the agency. Id. § 552a(g)(1)(D). And if the Court "determines that the agency acted in a manner which was

intentional or willful, the United States shall be liable in amount equal to the sum of . . . actual damages sustained by the individual as a result of the . . . failure.” Id. § 552a(g)(4)(A).⁴

As relevant here, the Privacy Act requires “actual—that is, pecuniary or material—harm.” FAA v. Cooper, 566 U.S. 284, 296 (2012). The United States retains sovereign immunity for non-economic harms, such as “loss of reputation, shame, mortification, injury to the feelings and the like.” Id. at 295–96, 299, 304. The D.C. Circuit has made clear that the purchase of “credit protection and/or credit repair services after learning of [a data] breach” is “the paradigmatic example of ‘actual damages’ resulting from the violation of privacy protections.” In re U.S. Off. Of Pers. Mgmt. Data. Sec. Breach Litig. 928 F.3d 42, 65 (D.C. Cir. 2019) (“In re OPM”) (citing Cooper, 566 U.S. at 298). Those costs must be “reasonably incurred.” Id. And the agency’s violation must be the “proximate cause” of any damages—that is, the violation “must have been a ‘substantial factor’ in the events leading to [plaintiffs’] injuries” and any injuries must have been “reasonably foreseeable” to the agency. Id. at 67 (citation omitted).

Defendants contend that Plaintiffs have not stated a claim under the Privacy Act because they have not alleged that they suffered actual damages. Before analyzing that contention against the allegations in the complaint, the Court makes three preliminary observations.

First, as Defendants emphasize, this case does not involve a cyberattack or other type of malicious incursion into Defendants’ computer systems. Whatever qualms Plaintiffs might have about DOGE staffers’ lack of clearance or training, they have not alleged facts indicating that DOGE staffers are malevolent actors akin to the foreign adversaries in In re OPM or hackers or

⁴ The Act entitles plaintiffs who succeed in their suit to a minimum award of \$1,000 as well as attorney fees and costs. 5 U.S.C. § 552a(g)(4)(A)–(B).

thieves in other Privacy Act cases. See e.g., Phillips v. U.S. Nuclear Regul. Comm’n, No. 24-cv-1999 (JEB), 2025 WL 958275, at *6–7 (D.D.C. Mar. 31, 2025) (concerning an alleged hack); Beck v. McDonald, 848 F.3d 262, 267–68 (4th Cir. 2017) (concerning the alleged theft of a laptop containing sensitive records and the alleged misplacement or theft of sensitive files). DOGE staffers reportedly were special government employees (albeit perhaps not yet onboarded in some cases), working within the executive branch. Therefore, Plaintiffs cannot justify the purchase of identity theft protection services on the ground that they were protecting themselves from the potential (or actual) consequences of a hack, as in In re OPM. Pls.’ Opp’n at 28.

Second, as noted above, one Plaintiff claims she experienced unauthorized debit charges following the sharing of her data with DOGE and another says he learned that his personal email address was found on the “dark web.” See FAC ¶¶ 83–85. But neither of these allegations offer sufficient facts to infer a causal connection between these occurrences and the DOGE disclosures. The Court therefore disregards them both as a potential independent form of damages and in assessing the reasonableness of the Plaintiffs’ purchase of identity theft protection.

Third, Defendants argue that the prophylactic measures Plaintiffs describe taking do not qualify as actual damages because Plaintiffs were not at “substantial risk” of their data being leaked due to the DOGE disclosures. See Defs.’ Mot. at 23 (quoting Stewart v. Kendall, 578 F. Supp. 3d 18, 24 (D.D.C. 2022)). But that standard for pleading actual damages has no basis in the Privacy Act. Indeed, the case Defendants cite to support the standard was dismissed for lack of standing, rather than a failure to state a claim under the Act. Stewart, 578 F. Supp. 3d at 25 (concluding that the plaintiff lacked standing to bring a claim based on the “hypothetical future harm” from a future data breach (citation omitted)). And though the D.C. Circuit has not

squarely addressed the issue, the Circuit applied the “substantial risk” standard only to Plaintiffs’ standing arguments in In re OPM. 928 F.3d at 55–61. By contrast, in analyzing whether those plaintiffs had suffered actual damages under the Act, the Circuit considered only whether the purchase of identity theft monitoring or protection services was “reasonable.” Id. at 65.

With that backdrop, the Court turns to the allegations in the complaint. For purposes of this motion at least, Defendants nowhere contest that a Privacy Act violation occurred. The Court therefore need not dally on the issue, except to say that the complaint alleges the unauthorized sharing of data with affiliates of DOGE, a willful violation of the Act.⁵ Likewise, Plaintiffs have clearly alleged that the sharing of data with DOGE was a substantial factor leading to the purchase of identity theft protection services; absent it, Plaintiffs would not have made the purchases, at least according to the complaint. See id. at 67. And it certainly should have been foreseeable to the agencies that sharing their data in the haphazard manner described in the complaint would have caused affected employees to be concerned about the security of their personal information. Id.

As to whether Plaintiffs have alleged sufficient facts to indicate that their decision to take prophylactic measures was reasonable, the Court, drawing every reasonable inference in their

⁵ DOGE had both a central headquarters and teams embedded in various agencies. The Privacy Act does not forbid sharing data within an agency, so long as the “officer or employee[]” has a “need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). Therefore, if the embedded DOGE team members can be considered employees or officers of OPM and Treasury, rather than of DOGE itself, it may be that the sharing of data with some individuals affiliated with DOGE was not a violation of the Act. But see Am. Fed’n of Lab. & Cong. of Indus. Orgs., 778 F. Supp. 3d at 83–84 (rejecting this argument). Regardless, Plaintiffs allege that the agencies shared data with at least some individuals who appear to have been a part of DOGE proper rather than members of an agency-embedded team. See e.g., FAC ¶¶ 30, 33–34. Defendants do not move to dismiss on these grounds in any case. The Court will therefore leave this issue for another day.

favor, finds that they have. The most relevant allegations on this front are as follows: First, Plaintiffs claim that their information was shared with individuals who were not government employees at the time, who had not undergone necessary training, and who had demonstrated a willingness to share data in an unsafe fashion, FAC ¶¶ 30–31, 33; they further allege that some DOGE staffers had limited work experience and that what experience they did have was with Mr. Musk and his companies, calling into question whether they should have been entrusted with preserving the security of government data, id. ¶ 34. Second, Plaintiffs indicate that they were aware of contemporaneous public expert reports about how changes in agency security protocols generally could lead to increased risk of improper data exfiltration. See, e.g., id. ¶ 48. Finally, and perhaps most critically, Plaintiffs point to their awareness of Mr. Berulis’s whistleblower disclosure to Congress, which noted that “suspicious log-in attempts to the NLRB’s secure systems were made by an IP address in Russia and there was a spike in data leaving the agency.” Id. ¶ 49. As noted above, Berulis posited that whoever was attempting to exfiltrate sensitive data “was using one of the newly created accounts that were used in the other DOGE related activities.” Id. ¶ 62 (citation omitted). And these events apparently followed soon on the heels of DOGE gaining full and unfettered access to the agency’s systems. Id. ¶¶ 50–54. The Court finds that a government employee who was aware of these warning signs and responded by purchasing identity-protection services did so reasonably.

The proof, in turns out, may have been in the pudding. Last month, in the ongoing AFSCME litigation in the District of Maryland, the government filed a “Notice of Corrections to the Record.” Among other things, the government acknowledged that DOGE officials had been given full access to systems and files containing sensitive individualized data and that at least one of them copied a non-SSA employee on an email that included a file that contained sensitive

information for roughly 1,000 people. See Notice of Recent Filing in Related Case (ECF No. 27), Ex. A at 2–4. Further, the government shared that DOGE had used third-party servers and that the government “has not been able to determine exactly what data were shared to [the server] or whether the data still exist on the server.” Id. at 6. Finally, the government revealed that

[a] political advocacy group contacted two members of SSA’s DOGE Team with a request to analyze state voter rolls that the advocacy group had acquired. The advocacy group’s stated aim was to find evidence of voter fraud and to overturn election results in certain States. In connection with these communications, one of the DOGE team members signed a “Voter Data Agreement,” in his capacity as an SSA employee, with the advocacy group. He sent the executed agreement to the advocacy group on March 24, 2025.

Id. at 5 (footnote omitted). Although the government does not indicate whether any data was shared under that agreement, these recent admissions tend to confirm Plaintiffs’ stated fears.

Their efforts to protect themselves have thus proven only more reasonable as time has passed.

Defendants try but fail to escape the conclusion Plaintiffs have pled actual damages. First, pointing to this Court’s ruling in Keown v. International Ass’n of Sheet Metal Air Rail Transportation Workers, No. 23-cv-3570 (CRC), 2024 WL 4239936, at *9 (D.D.C. Sept. 19, 2024), they argue that the heightened risk of misuse of personal information and lost time trying to rectify it do not qualify as actual damages. See Defs.’ Mot. at 24–25. But Keown concerned a negligence claim under District of Columbia law following a data breach of a private organization. See 2024 WL 4239936, at *9. Here, the governing law is the Privacy Act, which applies only to disclosures by the federal government and only to willful conduct. Moreover, the relevant plaintiff in Keown had yet to purchase identity-theft protection, unlike Plaintiffs here who did. Id. Keown is therefore distinguishable on both legal and factual grounds.

Defendants also urge that it is possible that the agencies did not disclose Plaintiffs’ data specifically, thereby breaking the connection between the alleged violation of the Act and

Plaintiffs’ prophylactic measures. See Defs.’ Mot. at 25–26. At the motion to dismiss stage, however, the Court must give every reasonable inference to Plaintiffs. And it is reasonable to infer that the agencies disclosed their particular data to DOGE given the public reports about DOGE’s access to agency databases described in the complaint.

Relatedly, Defendants suggest that Plaintiffs should be required to show that DOGE staffers actually viewed their data for a Privacy Act disclosure to have occurred. See id. at 26 (collecting cases). But the D.C. Circuit has generally rejected such a cramped reading of “disclose” in the Act. See Pilon v. U.S. Dep’t of Just., 73 F.3d 1111, 1118 (D.C. Cir. 1996) (collecting definitions from dictionaries and other statutes indicating that “disclose” in the Privacy Act “encompass[es] the act of exposing or disseminating an item”); see also 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.”). And when “interpreting the terms of the Privacy Act *specifically*,” the Circuit has “taken particular care not to undermine the Act’s fundamental goals.” Pilon, 73 F.3d at 1118. The Court declines to read “disclose” in such a way that might contradict prior D.C. Circuit holdings on both the term’s meaning and how to interpret the Privacy Act generally.

III. Conclusion

For the foregoing reasons, it is hereby

ORDERED that [22] Defendants’ Motion to Dismiss Plaintiffs’ Amended Complaint is hereby DENIED. It is further

ORDERED that Defendants shall answer Plaintiffs’ First Amended Class Action Complaint by April 3, 2026.

SO ORDERED.



CHRISTOPHER R. COOPER
United States District Judge

Date: March 4, 2026