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' REPLY IN SUPPORT OF MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Other Authorities

INTRODUCTION

At its core, the Amended Complaint contains no credible allegations of a data breach, or any disclosure of Plaintiffs' PSI to those outside of the government. Plaintiffs leans on a body of data breach precedent that presupposes criminal exfiltration or public dissemination of personal data. *See generally* Opposition to Defendants' Motion to Dismiss the First Amended Complaint ("Pls.' Resp."), ECF No. 24. This case plausibly alleges neither. At most, the Amended Complaint posits disclosure of agency records to government personnel. This is a far cry from a data breach perpetrated by criminals, as Plaintiffs readily allege. *See Barclift v. Keystone Cred. Servs.,* LLC, 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.").

Plaintiffs continuously remind this Court that their pleading must be accepted "as true," Pls.' Resp. at 7, 22, 27, and that they need not prove that a data breach has taken place yet because that is the very purpose of discovery, *id.* at 21. But Plaintiffs forget that they 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) (emphasis added) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Plaintiffs must go beyond "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements"; barebones pleadings "do not suffice." *Id.*

There is no plausible allegation of theft, publication to bad actors, or misuse of any named Plaintiffs' information traceable to Defendants. Indeed, Plaintiffs can cite to no authority holding that intra-governmental, internal access to records constitutes a "data breach"—and none of their cases involving USDS or any other entity say otherwise. Their repeated effort to rebrand internal sharing of information as a criminal exfiltration defies both logic and the caselaw, which deals with actual cybersecurity breaches by third-party hackers and nefarious actors. Under *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), and *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), that ends the Article III inquiry.

The authorities Plaintiffs cite (*e.g.*, *Attias*, *Equifax*, *Marriott*, *Zappos*) are telling. They involve circumstances evincing criminal exfiltration of consumers' PSI—facts courts found sufficient to establish a substantial risk of identity theft. Nothing similar is plausibly alleged here. Plaintiffs plead only access by USDS personnel. They identify no third-party criminal, no dark-web sale of their Social Security or bank data, and no plausible causal bridge between Defendants and the few scattered anecdotes of fraud they invoke. Those anecdotes look far more like the ubiquitous fraudulent credit and debit card purchases rejected as too speculative in cases like *SAIC*. *See In re Sci. Applications Int'l Corp. ("SAIC") Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31 (D.D.C. 2014). Plaintiffs nevertheless contend that three isolated, unauthorized purchases are traceable to Defendant agency's conduct. But this again amounts to pure conjecture, particularly when, just last year, more than 62 million Americans experienced credit card fraud. Brett Cruz, *62 Million Americans Experienced Credit Card Fraud Last Year*, Security.org (Jan. 27, 2025), https://perma.cc/KEM2-DFSZ.

Plaintiffs' Privacy Act claim fares no better. Under *FAA v. Cooper*, and *Doe v. Chao,* pecuniary loss is required to state a claim. 566 U.S. 284, 290 (2012); 540 U.S. 614, 620-27 (2004). Purchasing identity theft protection services based on bare speculation that some harm might happen in the future does not rise to the sufficient "substantial risk" called for to find that mitigation costs can amount to pecuniary harm. *Clapper*, 568 U.S. at 414 n.5; *see Stewart v. Kendall*, 578 F. Supp. 3d 18, 23-24 (D.D.C. 2022). Indeed, all Plaintiffs purchased identity theft protection services before any alleged fraudulent credit or debit purchases occurred, or any publication on the dark web of their innocuous personal information such as their personal email. Just as in *Clapper*, "allowing [Plaintiffs] to bring this action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of [Plaintiffs'] first failed theory of standing." 568 U.S. at 416.

Plaintiffs' brief is also replete with mischaracterizations of Defendants' arguments, hollow distinctions, and citations to inapposite cases that nearly all involve either stolen or exfiltrated data.

Finally, the Supreme Court recently granted the government's application for a stay of a district court's preliminary injunction order in another case challenging USDS's access to agency records systems under the Privacy Act. *Soc. Sec. Admin. v. Am. Fed'n of State, Cnty., & Mun. Emps.*, 145 S. Ct. 1626 (2025) ("*SSA*"). Although this order was not based on the merits, it strongly militates towards finding in favor of the Defendants here as the claims and facts in the stayed case are highly analogous, if not functionally indistinguishable. This Court should follow suit.

ARGUMENT

I. Plaintiffs Lack Standing

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

1. Plaintiffs' Alleged Injury Is Not Cognizable In Common Law

Plaintiffs have little response to the threshold issue of whether their claimed injury is analogous to a harm recognized in the common law. Primarily, Plaintiffs argue that the government relies only on out-of-circuit appellate authority, *Am. Fed'n of Tchrs. v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025), rather than a district court opinion within this circuit. Pls.' Resp. at 13-14. But the Supreme Court has since vacated a preliminary injunction premised on the same theory of standing that Plaintiffs posit here.

In *American Federation of Teachers v. Bessent*, plaintiffs claimed violations of the Privacy Act and the APA when the Department of the Treasury and the Department of Education granted USDS access to agency records, and plaintiffs' PSI. 772 F. Supp. 3d 608 (D. Md. 2025), *vacated and remanded*, No. 25-1282, 2025 WL 2313244 (4th Cir. Aug. 12, 2025). The district court concluded that intrusion upon seclusion served as a sufficiently close common law analogue. *Id.* at 630-33. The Fourth Circuit disagreed. *Id.* The Fourth Circuit held that plaintiffs lacked standing as plaintiffs did not experience an injury similar to the harm of intrusion upon seclusion. *Am. Fed'n of Tchrs. v. Bessent*, No. 25-1282, 2025 WL 2313244 at *6 (4th Cir. Aug. 12, 2025).

In *SSA*, the Supreme Court stayed the district court's injunction that enjoined the Social Security Administration from granting its USDS team access to agency systems. 145 S. Ct. 1626.

The Supreme Court concluded that consideration of the *Nken* factors "warrants granting [a] . . . stay," and that "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." *Id.* (citing *Nken v. Holder*, 556 U.S. 418, 434 (2009)). This Court should heed the recent signals from the Supreme Court and the Fourth Circuit that suggest claims like these—based on such abstract, intangible injuries—cannot proceed. *Cf., Trump v. Boyle*, 145 S. Ct. 2653, 2654 (2025) ("Although [the Supreme Court's] interim orders are not conclusive as to the merits, they inform how a court should exercise its equitable discretion in like cases.").

In a footnote, Plaintiffs address this intervening precedent, and claim that all that can be gleaned from *SSA* is that "the Supreme Court had some concern about the preliminary injunction at issue[.]" Pls.' Resp. at 14 n.5. Justice Gorsuch, however, has noted that "even probabilistic holdings—such as *California*'s[1] top-line conclusion that 'the Government is likely to succeed in showing the District Court lacked jurisdiction to order the payment of money under the APA,' must 'inform how a [lower] court' proceeds 'in like cases[.]'" *Nat'l Insts. of Health v. Am. Pub. Health Ass'n*, 145 S. Ct. 2658, 2664 (2025) (citations omitted). So too here. Given that the Supreme Court has already stayed a preliminary injunction in a materially similar case, this Court should follow suit and dismiss Plaintiffs' Amended Complaint.

Recognizing that the theory of "intrusion upon seclusion" did not appear to persuade the Supreme Court, Plaintiffs shift their approach to argue "breach of confidence." Pls.' Resp. at 15. But this theory fails as well. Plaintiffs rely exclusively on the one recent decision in which a court relied on this particular tort. *See Am. Fed'n of Lab. & Cong. of Indus. Orgs. v. Dep't of Lab.*, 778 F. Supp. 3d 56, 73 (D.D.C. 2025) ("*AFL*") (quoting *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1064 (D.C. Cir. 2019)). But it is highly unlikely that this tort qualifies as a traditional cause of action. *See TransUnion*, 594 U.S. at 427 (starting that "lawsuit may not proceed because that

[1] This matter, like *SSA*, stayed the district court's preliminary injunction order. *See generally Dep't of Educ. v. California*, 604 U.S. 650 (2025).

plaintiff has not suffered any . . . harm *traditionally* recognized as providing a basis for a lawsuit in American courts" (emphasis added)).

While the D.C. Circuit in *Jeffries* invoked the tort to find standing, that decision predates *TransUnion*, does not specifically address whether the tort has a sufficient historical origin and relies extensively on an Eleventh Circuit panel decision that was later overturned by the Eleventh Circuit sitting en banc. *See Jeffries*, 928 F.3d at 1064–65 (citing *Muransky v. Godiva Chocolatier, Inc.*, 922 F.3d 1175 (11th Cir. 2019), *reh'g en banc granted, opinion vacated*, 939 F.3d 1278 (11th Cir. 2019), and *on reh'g en banc*, 979 F.3d 917 (11th Cir. 2020)). In that en banc decision, which came out after *Jeffries*, the Eleventh Circuit questioned, without deciding, whether breach of confidence "can fairly be said to have 'traditionally been regarded as providing a basis for a lawsuit in English or American courts'" for standing purposes. *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc) (quoting *Spokeo v. Robins*, 578 U.S. 330, 341 (2016)). The Eleventh Circuit found that the tort has been "emerging" only since the 1980s in a "rudimentary form after initially dying out in its infancy." *Id.* (citation modified).

The Second Circuit has described it as a "a relative newcomer to the tort family" and found that the tort is usually limited to the physician-patient or bank-customer relationships. *Young v. U.S. Dep't of Just.*, 882 F.2d 633, 640 (2d Cir. 1989). The tort's nascent and underdeveloped pedigree raises serious doubts about whether this tort can serve as a valid analogue under *TransUnion*'s requirement of a historically grounded cause of action.

Even assuming that the breach of confidence tort is a permissible analogue for standing purposes, the facts here bear little resemblance to the typical circumstances where it applies: the physician-patient or bank-customer relationships. *Young*, 882 F.2d at 640. In *Jeffries*, the D.C. Circuit analogized it to a situation involving unauthorized disclosure of credit card information, which would be similar to the bank-customer framework. 928 F.3d at 1064. This case, by contrast, does not involve a financial institution nor inherently financial information—it involves a federal

agency and employee information. And this case is most certainly not analogous to the physician-patient relationship.

And even if this Court were to apply the elements of the tort, the analogy still falls flat. The tort "lies whe[n] a person offers private information to a third party in confidence and the third party reveals that information to another." *AFL*, 778 F. Supp. 3d at 73 (quoting *Jeffries*, 928 F.3d at 1064). The elements of the tort are not comparable to the situation here. Plaintiffs do not plausibly allege that any of its members' information was actually accessed by or directly shared with any USDS personnel. But more so, as the Executive Order establishes, agency personnel comprise current personnel or new hires "*within* their respective Agencies." *See* Establishing and Implementing the President's "Department of Government Efficiency," Exec. Order No. 14158 § 3(c), 90 Fed. Reg. 8441 (Jan. 20, 2025) (emphasis added). Thus, any reliance on the tort of breach of confidence necessarily fails, as the information is not being shared with "another" but simply with agency employees.

2. Plaintiffs' Alleged Injuries Are Not Concrete Harms

Plaintiffs spend much of their opposition insisting that they have suffered actual injury. Pls.' Resp. at 16-21. But this supposed actual injury is nothing more than speculation untethered to allegations of fact.

First, Plaintiffs allege "actual misuse" of their PSI. *Id.* at 9. This misuse allegedly arises from allegations by Plaintiffs Nemeth and Nemeth-Greenleaf that fraudulent purchases were made with their credit card and debit card and that they and that Plaintiffs Nemeth-Greenleaf and Rifer were notified that some of the same information submitted to the agencies appeared on the dark web. *Id*. at 9-11. In support of this claim, they cite *In re U.S. Office of Personnel Management Data Security Breach Litigation* ("*In re OPM*"), for the proposition that identity theft constitutes a concrete and particularized injury. 928 F.3d 42, 55 (D.C. Cir. 2019); Pls.' Resp. at 9. Defendants do not and have not contested that identity theft can constitute a concrete Article III injury. What Defendants *have* contested (at length) is that Plaintiffs have not plausibly alleged that their

specified instance of identity theft, here the unauthorized credit and debit card purchases, are plausibly traceable to Defendant agencies. *See* Mem. of Law in Supp. of Defs.' Mot. to Dismiss Pls.' Am. Compl. ("Def.'s Mot.") at 17-20, 27, ECF No. 22; *infra* Part I.B.

Plaintiffs rely on *Hancock v. Urban Outfitters, Inc.*, to establish that "increased risk of fraud or identity theft" is an example of a concrete injury. 830 F.3d 511, 514 (D.C. Cir. 2016); Pls.' Resp. at 15. But Plaintiffs utterly fail, however, to connect ordinary credit card fraud to the intra-agency transfer of information at issue here. *See* Def.'s Mot. at 26-31; 35; *infra* I.B. Even if Plaintiffs could credibly allege that the information they aver was in Defendants' control had somehow been disclosed to a nefarious actor, (which they cannot), the information is insufficient to execute the three instances of fraudulent purchases that Plaintiffs contend is the cornerstone of their claim to actual harm. *See* Def.'s Mot. at 27 (To successfully execute the fraudulent purchases, the criminal would have likely had to have obtained access to their "credit card number, personal identification numbers ("PINs"), card verification value code ("CVV"), expiration date, billing address, and perhaps a host of answers to security questions." (citing Mark Kapczynski, *What can someone do with your account and routing number?*, OneRep (June 12, 2025), https://perma.cc/3BLQ-6NFT)); *see How To Protect Yourself From Credit Card Fraud*, Unify, https://perma.cc/QM7H-UK94 (last accessed Sept. 25, 2025). Plaintiffs have not alleged that each piece of the necessary information was in Defendants' possession. Nor do they rebut, (apart from a passing claim that it "defies simple common sense" that an identity thief could not make the purchases with the information in Defendants' possession), that such information would have been needed to enable the fraudulent purchases. Pls.' Resp. at 33. And most critically, Plaintiffs allege no plausible causal connection to OPM and Treasury, since they fail to allege that *only* OPM and Treasury possessed these Plaintiffs' PSI.

Second, Plaintiffs allege that Defendants' actions placed them at imminent risk of identity theft. *Id.* at 10. But despite their insistence that "important context," *id.*, describing cyber intrusions at *other* federal agencies necessarily places their PSI at imminent risk of identity theft,

such conjecture is classically insufficient to claim Article III standing, *Clapper*, 568 U.S. at 413-14. Indeed, if a plaintiff could bring a Privacy Act claim on the premise that other agencies have experienced cybersecurity breaches, and therefore their own information must be in peril, every government employee would have a viable claim under the Privacy Act. Their assumption that a cybercriminal would necessarily target their information next as a result of prior breaches amounts to bare speculation. *Id.* at 411 ("[I]t is [highly] speculative whether the Government will imminently target communications to which respondents are parties.").

Indeed, Plaintiffs fail to explain any possible connection to the fact that over ten years ago OPM experienced a data breach, and their claim that they are now at imminent risk of a similar or related breach. First Am. Class Action Compl. ("Am. Compl.") ¶ 47, ECF No. 19. The mere fact that a breach occurred in the past does not mean it is likely to happen again. *Stewart*, 578 F. Supp. 3d at 24 ("Plaintiff brings no allegations about the potential threat of a repeat breach" and that the "mere fact that a breach happened in the past does not mean it is likely to happen again in the future."). Indeed, nowhere do Plaintiffs credibly allege that such a risk, however remote or implausible, is imminent (a requirement for alleged future harm). *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 381 (2024). Neither do any of Plaintiffs' purported contextual explanations lead one to surmise that Plaintiffs' predictions are anything more than bare speculation. *See Clapper*, 568 U.S. at 409 (For an injury to be imminent, it must be "certainly impending;" mere "allegations of possible future injury are not sufficient." (citation modified)); Pls.' Resp. at 15-17.

Third, Plaintiffs assert that emotional harm, such as fear and anxiety resulting from a possible unlawful disclosure of PSI, is sufficient to confer standing. Pls.' Resp. at 12. The three cases they rely on to support this claim, however, are inapt, as none examined the Privacy Act. Under the Privacy Act, emotional harm is not cognizable. Instead, the Privacy Act requires Plaintiffs to plead "actual damages," that is "pecuniary harm[.]" *Cooper*, 566 U.S. at 287, 295-96 (citation omitted). *Cooper* expressly instructs there is no waiver of sovereign immunity under the Privacy Act for damages relating to mental or emotional distress. *Id*. at 287, 295-96; *see also*

Welborn v. Internal Revenue Serv., 218 F. Supp. 3d 64, 82 (D.D.C. 2016) (finding that "[t]he Privacy Act does not allow a claim for damages based on . . . emotional harm[,]" and "Plaintiff[] must specifically allege actual damages to survive a motion to dismiss for failure to state a claim.").

Last, Plaintiffs suggest that the time spent and costs incurred to mitigate potential harms, here—the purchase of identity theft prevention services—are recognized as concrete injuries that support Article III standing. But for mitigation costs to qualify as actual damages, there must be at least a *substantial risk* of future harm justifying the outlay of time and money.[2] *Stewart*, 578 F. Supp.3d at 24. Plaintiffs have not sufficiently alleged that such mitigation costs were made in reasonable reaction to a substantial risk of identity theft. *See* Def.'s Mot. at 23-26. There is no plausible substantial risk of future harm to Plaintiffs' PSI because there has been no actual data breach of Plaintiffs' information to criminals or the public, and Plaintiffs have not plausibly alleged that such a breach is imminently likely.

This case, moreover, is nothing like cases where a substantial risk of future harm were found. In *Attias v. Carefirst, Inc.*, a health insurance provider "suffered a cyberattack" in which customers' personal information was stolen. 865 F.3d 620, 622 (D.C. Cir. 2017). The panel found that the plaintiffs plausibly alleged that they "face a substantial risk of identity theft as a result of [the provider's] alleged negligence" because the breach "exposed [their] social security and credit card numbers" to an intruder. *Id.* at 627–28. Because the breach had already happened, "an unauthorized party had already accessed" personal data and it was "plausible . . . to infer that this party has both the intent and the ability to use that data for ill." *Id.* at 628. Similarly, in *In re OPM*, plaintiffs asserted that a widespread data breach that exposed their personal information

---

[2] Plaintiffs cite four cases to support the opposite conclusion. Pls.' Resp. at 12-13. Generally, each case stands for the argument that time and money spent mitigating the effects of a data breach constitute an injury. But none of the cases were brought under the Privacy Act. Because Plaintiffs must uniquely prove "actual damages" (pecuniary damages), the Act's scheme only recognizes certain forms of injury as sufficient to plead a Privacy Act claim. Here, Plaintiffs would need to find such mitigation costs constituted "actual damages."

(including Social Security numbers, birth dates, residency details, and fingerprints) made them susceptible to the risk of future fraud and identity theft. 928 F.3d at 58–59. The Circuit agreed and found that the costs incurred by purchasing credit-monitoring services, along with other mitigation costs, qualified as an injury-in-fact. *Id.* at 60.

Here, "plaintiff [] does not allege that because of the Privacy Act violation his personal information is currently in the hands of a malicious actor seeking to steal his identity." *Stewart*, 578 F. Supp. 3d at 25. Plaintiffs cannot allege beyond conclusory statements that any of their PSI is in the hands of a malicious actor. *See Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021) ("[Plaintiff] offers only vague, conclusory allegations that members of the class have suffered any actual misuse of their personal data—here, 'unauthorized charges.' But again, conclusory allegations of injury are not enough to confer standing."). As discussed above, it is purely speculative whether the alleged access provided to USDS team members within agencies will result in any outside disclosure of data, let alone theft of Plaintiffs' identity. 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 Just.*, 279 F. Supp. 3d 279 (D.D.C. 2017) (emphasis omitted) (quoting *Cooper*, 566 U.S. at 299).

Plaintiffs' attempt to rely on mitigation expenses also fail due to the timing of those expenditures. Plaintiffs purchased the credit monitoring and identity theft protection services identified in their original Complaint *before* they alleged any theory of actual harm stemming from the unauthorized credit and debit card purchases. *See* Compl., ¶¶ 19-23, ECF No. 1. Any mitigation costs or time and effort incurred were plainly not made in response to a substantial risk of future identity theft or a data breach. *See Randolph v. ING Life Ins. & Annuity Co*., 973 A.2d 702, 708 (D.D.C. 2009) ("[T]o the extent that appellants allege actual harm from expenses they have incurred to undertake credit monitoring or other security measures to guard against possible misuse of their data," they have "alleged an injury that is 'not the result of any present injury, but

rather the [result of] the anticipation of future injury that has not materialized.'" (quoting *Randolph v. ING Life Ins. & Annuity Co.*, 486 F.Supp.2d 1, 8 (D.D.C. 2007))).

Plaintiffs' efforts to characterize their allegations as anything but speculation fall flat. *See, e.g.* Def.'s Mot. at 13-17. Plaintiffs need not be "literally certain," Pls.' Resp. at 16, that their data will be misused, but they must plausibly allege that their future harms are likely and not speculative. This they cannot do. A plaintiff alleging a threat of harm does not have Article III standing unless the hypothetical harm alleged is either "certainly impending" or there is a "substantial risk" of such harm. *Clapper*, 568 U.S. at 409, 414 n.5. And if the hypothetical harm alleged is not "certainly impending," or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk. *Id.* at 416.

Plaintiffs state that allegations of misuse of their PSI are "sufficient to substantiate a risk of future harm on all the named Plaintiffs." Pls.' Resp. at 17. But the cases Plaintiffs cite bear no resemblance to the facts here either. Each of the cited cases involved an undisputed cyberattack or data breach. Facts markedly absent at present. Take for example *In re Equifax Inc. Customer Data Security Breach Litigation*, 999 F.3d 1247, 1263 (11th Cir. 2021). There the court found that an undisputed data breach by nefarious actors (not present here), in a case involving one of the largest data breaches in recent memory, *did* pose a substantial risk of future harm. *Id*. at 1262 ("[H]ackers obtained at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers." (citation omitted)). While the plaintiffs in *Equifax* alleged that they had incurred numerous fraudulent credit card charges, *Id*. at 1262-63, Plaintiffs here do not credibly allege that any of their information has been made public. Or that any of the information that Plaintiffs allege were in Defendants' possession could be used to complete the unauthorized transactions.

Similarly, in *In re Marriott International, Inc., Customer Data Security Breach Litigation*, 440 F. Supp. 3d 447, 459 (D. Md. 2020), Marriott was targeted with "one of the largest sustained cyberattacks in history" that compromised the PSI of up to 500 million hotel guests. That is a far cry from the present facts, where it bears repeating that Plaintiffs have not credibly alleged any data breach where their information has been made public. Likewise, in *In re Mednax Services, Inc. Customer Data Security Breach Litigation*, 603 F. Supp. 3d 1183, 1203 (S.D. Fla. 2022), there was again an actual data breach where unknown third parties gained access to plaintiffs information. Plaintiffs' theory rests on a highly speculative chain of events premised on the assumption that—because USDS personnel have access to Defendants' information, that they somehow released said information to the public or to a nefarious actor, and that nefarious actor in turn was the culprit of the three unauthorized charges experienced by two Plaintiffs. Such a chain of specious hypotheticals falls well short of establishing any "substantial risk" to their information.

Plaintiffs also claim that their allegations are "akin to those in *AFL*." Pls.' Resp. at 18 (citing 778 F. Supp. 3d at 69–70). Not so. They attest that the court there found that when DOL leadership directed agency employees to give USDS personnel access to DOL systems, and when HHS granted USDS personnel access to such systems, that such harm was "imminent." *Id.* at 23. Plaintiffs then conclude that "[i]t takes no chain of speculation to conclude from these allegations that [Defendants] are providing [USDS] personnel access to systems that contain plaintiffs' [PSI]." *Id.* (quoting *AFL*, 778 F. Supp. 3d at 70). They also include a footnote, *id*. at 18 n.9, stating that for this reason, "Defendants' conclusory citations on this point are inapposite."

Plaintiffs' position rests on a gap in reasoning. Plaintiffs' citation to *AFL* causally connects allegations (of USDS personnel's access to systems containing plaintiffs' PSI) to the alleged harm in that case (that USDS personnel have access to plaintiffs' PSI). That may have been the crux of the alleged harm in *AFL*. But that is not the case here. Here, the allegations are the same, *i.e*., that USDS personnel were given access to Plaintiffs' PSI. But the alleged harm is entirely different.

The thrust of Plaintiffs' theory of harm does not stop at the alleged harm in the *AFL* case, but goes further, and alleges that *because* USDS personnel obtained access to their information, that such access will make them "vulnerable to fraud, cyber-attack, and actual theft" and will put them at "extreme risk that such data would fall and has fallen into the hands of third party bad actors, including foreign adversaries" and that identity theft occurred as a result. Am. Compl. ¶¶ 71, 78-79; Pls.' Resp. at 27.

This attempted analogy to *AFL* fails. The theory of harm there was carefully circumscribed, while here it amounts to boundless speculation. Put another way: whereas in *AFL* plaintiffs alleged that USDS personnel's access to plaintiffs' PSI was itself a harm, here Plaintiffs speculate that alleged USDS access will necessarily result or has resulted in a data breach that will make Plaintiffs imminently vulnerable to identity theft. The analogy collapses as the harms are mismatched. Indeed, if anything, the disparity militates against Plaintiffs by confirming the speculative nature of their claims.

Plaintiffs attack cases cited by Defendants as "either inapplicable here or actually support[ing] Plaintiffs' claims." Pls.' Resp. at 19. They conclude, for example, that *Doe v. Office of Personnel Management*, No. CV 25-234 (RDM), 2025 WL 513268 (D.D.C. Feb. 17, 2025) is inapposite, because it did not involve a Privacy Act claim or any improper disclosure. *Id.* But this is exactly the point. A Privacy Act claim or allegations of improper disclosure could not be brought because in *Doe*, as here, there has been no unlawful public exposure of their PSI. *Doe*, 2025 WL 513268 at *6 ("Although an *actual* hacking incident or an imminent hack might suffice, Article III requires more than a possibility of future harm—a 'theory of future injury' must be "'certainly impending' and non-speculative." (emphasis added) (quoting *Clapper*, 568 U.S. at 401)). Plaintiffs next insist that Defendants' citation to *University of California Student Ass'n v. Carter*, 766 F. Supp. 3d 114 (D.D.C. 2025) is "puzzling" and "dubious." Pls.' Resp. at 19. But Plaintiffs are again attacking a strawman of their own making. Not once did Defendants cite that case as a dispositive authority on standing. Def.'s Mot. at 15-16. Instead, it was cited for the proposition

that allegations of harm in that case, similar to here, amounted to "sheer speculation[.]" *Carter*, 766 F. Supp. 3d at 122.

Plaintiffs also claim that *American Federation of State, County & Municipal Employees, AFL-CIO v. Social Security Administration*, 771 F. Supp. 3d 717 (D. Md. 2025) ("*AFL-CIO*") does not help Defendants. Plaintiffs are incorrect, and their contention that "the court expressly distinguished its holding finding no standing from that in *New York v. Trump*," Def.'s Mot. at 20, is also misplaced. The *AFL-CIO* court never distinguished its finding but instead said that they recognize that the *New York* case "reach[ed] a different result[,]" *id*. at 770, 772 ("At this juncture, I am not prepared to speculate that the actions at issue will result in a data breach, and that a breach will necessarily result in identity theft. This concern is not sufficient to satisfy the demands of Article III.").

Plaintiffs' other attempts to devalue applicable cases also do not withstand scrutiny. They attack *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), because there the court ruled on standing after discovery. This is a distinction without a difference. First, district courts at the pleading stage regularly rely on other courts' holdings related to standing that take place after discovery. Indeed, the court in *AFL-CIO* stated, without qualification, that for standing: "I am guided by *Beck*, 848 F.3d 262." *AFL-CIO*, 771 F. Supp. 3d at 771. Second, the plaintiffs in *Beck* only reached discovery because there was an *actual* data breach, unlike here, that resulted from the theft of a laptop contains unencrypted personal information of approximately 7,400 patients and thus made their claim plausible enough so as to survive dismissal. *Beck*, 848 F.3d at 267. Plaintiffs also claim that *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009) is not apropos because in that case the plaintiff appeared to concede that there has been no publication of any information wrongfully obtained, allegedly unlike the current case. But to be clear, beyond the sweeping legal conclusions that Plaintiffs would prefer this Court take as true, Plaintiffs do not credibly allege that there has been *any* publication of information held by Defendant agencies. Their razor thin attempts at distinguishing this case from those cited are unavailing.

Last, Plaintiffs attempt to frame their allegations as not speculative merely because they have not yet proven that USDS and others have read Plaintiffs' individual data. Pls.' Resp. at 21. But again, this misses the point. Plaintiffs cannot even reach that determination because their claim is neither plausibly nor credibly alleged and is subject to dismissal for that reason. That stands in sharp contrast to nearly every case Plaintiffs cite, each of which involved "an actual hacking incident." *Doe*, 2025 WL 513268 at *6.

B. Plaintiffs' Alleged Harms Are Not Traceable To The Defendant Agencies

Plaintiffs dispute Defendants' arguments that the alleged unauthorized charges on their debit and credit cards and posting of personal emails on the dark web are not credibly traceable to Defendants' actions.

To start, Plaintiffs claim that Defendants' traceability standard is too strict for this stage in the proceedings and that Defendants conflate the merits of Plaintiffs' claims with standing. This is incorrect. The "injury [must] be fairly traceable to the challenged action of the defendant." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citation omitted); Def.'s Mot. at 17. Plaintiffs insist that Defendants' claim that Plaintiffs have failed to allege any public disclosure or data breach of their PSI beyond mere speculation ignores their "well-pled allegations." Def.'s Mot. at 22. But Plaintiffs' preferred standard, where allegations are taken at face value, is not the law. Plaintiffs must provide enough factual content to "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. This is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.* at 679. And the Court should "disregard rote recitals of the elements of a cause of action, legal conclusions, and mere conclusory statements." *James v. City of Wilkes-Barre*, 700 F.3d 675, 679 (3d Cir. 2012).

Plaintiffs contend that an alleged public disclosure took place when USDS personnel allegedly accessed agency information. But Plaintiffs muddle the inquiry. Plaintiffs equate USDS access to information as equivalent to a data breach. At most, this is an intra-governmental

disclosure made to other government employees. And even if we did assume that there was an impermissible disclosure, a disclosure to USDS personnel cannot credibly be deemed to be akin to a data breach or an attack by "hackers." *See* Am. Compl. ¶ 4. In any event, notwithstanding the implausible string of assumptions that Plaintiffs advance in equating USDS access as a public disclosure, "the courts must presume" that the government will exercise its powers "responsibly" and with "due regard" to affected individuals. *Ashland Oil, Inc. v. FTC*, 409 F. Supp. 297, 308 (D.D.C. 1976), *aff'd*, 548 F.2d 977 (D.C. Cir. 1976). This "presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties." *United States v. Chem. Found.*, 272 U.S. 1, 14–15 (1926).

Plaintiffs contend (albeit somewhat obscurely) that Defendants "contradict Plaintiffs' allegations that these disclosures to unauthorized persons exposed Plaintiffs' PSI to third-party bad actors" and to "substantial risk of future harm as to all Plaintiffs." Pls.' Resp. at 22–23. In support, they cite *AFL*: ("It takes no chain of speculation to conclude from these allegations that [Defendants] are providing [USDS] personnel access to systems that contain plaintiffs' members' [PSI]." (quoting *AFL*, 778 F. Supp. at 56)). But here, as stated above, *supra* at 12-13, there is a fundamental mismatch in Plaintiffs' attempt at analogizing their situation with that in *AFL*.

Plaintiffs next attempt to reframe Defendants' motion by citing arguments Defendants never made. Plaintiffs claim that Defendants stated that the PSI at issue is "so innocuous" that "even if disclosed, it could not be used to harm Plaintiffs." Pls.' Resp. at 23. This is not what Defendants said. Defendants wrote that "such relatively innocuous disclosures of PSI [alleged harms—personal emails and credit card information] are commonplace and cannot be credibly traced to any breach at Treasury at OPM, which is perhaps why Plaintiffs do not directly advance that there has been any public breach of their PSI by the Defendant agencies." Def.'s Mot. at 19. Again, Plaintiffs miss the mark when they claim that Defendants disclosed far more than "mere 'publicly available' information." Pls.' Resp. at 23. Defendants only stated that, with regard to

information allegedly posted on the dark web, the disclosure of "non-sensitive information, such as here, . . . have been repeatedly dismissed as a matter of course." Def.'s Mot. at 19.

Plaintiffs also cite *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 386 (6th Cir. 2016). In that case, plaintiffs had standing to bring data breach claims when the leaked information included "names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers." *Id*. But again, unlike there, where an actual data breach did occur, here, there has been no public dissemination of Plaintiffs' information beyond their bare speculation. Similarly, Plaintiffs' attempt to distinguish their case from *SAIC* also fails for the simple reason that they again cannot plausibly allege any public access of their information by nefarious actors. 45 F. Supp. 3d at 31-32.

Plaintiffs reliance on *In re OPM* fails for the same reason. That case also dealt with an *actual* data breach. 928 F.3d at 52 (arising out of cyberattacks that were "sophisticated, malicious, and carried out to obtain sensitive information for improper use."). In like manner, Plaintiffs state that "many courts have rejected motions to dismiss that raise similar challenges in *data breach cases* where resolving the issue involves factual inquiry, as it would here." Pls.' Resp. at 25 (emphasis added). The flaw in Plaintiffs' argument is apparent. Every case they cite involved an actual data breach. This case does not.

Last, Plaintiffs' claim that "[a]s Defendants make no mention of Plaintiffs Judkins and Michel, Defendants entirely fail to carry their burden on the instant motion to dismiss their claims for lack of traceability" also fails. *Id.* at 24 n.16. Defendants need not address those Plaintiffs' traceability of their alleged harm to the agency's actions because they do not claim any actual misuse of their PSI. It belies logic for Defendants to attempt to trace *fear* that their PSI will be misused in the future to any agency action. In any event, even with the three plaintiffs equipped with allegations of actual misuse, those allegations are conclusory and not plausible for all the reasons stated.

II. Plaintiffs' Privacy Act Claim Should Be Dismissed

***Mitigation Costs*:** Moving to the Privacy Act's mandate that pecuniary harm be found for any liability to accrue—Plaintiffs again ascribe to Defendants a position that they have not taken. Plaintiff state that "Defendants further claim that not only do such costs [mitigation costs] generally do not qualify as pecuniary harm . . . ." Defendants have not stated this. Instead, Defendants clearly state the relevant standard: that mitigation costs can qualify as pecuniary harm under the Privacy Act if such costs were made in response to a "substantial risk of future harm." Def.'s Mot. at 23; *see also Stewart*, 578 F. Supp. 3d at 24.

Plaintiffs continue their attempt to claim mitigation costs as pecuniary harm by citing *In re OPM,* 928 F.3d as an authority in support of their case. Pls.' Resp. at 27-28. Plaintiffs correctly surmise that the D.C. Circuit held in that matter that the "costs of credit protection and/or credit repair services following a data breach 'are the paradigmatic example of actual damages resulting from the violation of privacy protections.'" *Id*. (quoting *In re OPM*, 928 F.3d at 65). Yet again, however, Plaintiffs overlook that in that case—unlike here—there was an uncontested, *actual* data breach, with information made public to nefarious actors, that placed affected persons at substantial risk of future harm.

Plaintiffs contend that *In re OPM* is squarely on point because "Plaintiffs' very allegations in this action are that the Government unlawfully disclosed their personal information to unauthorized third parties—i.e., that an actual data breach occurred." Pls.' Resp. at 28 (emphasis omitted). Plaintiffs' argument strains credulity. Plaintiffs continue to labor under the misconception that their case resembles a data breach. Plaintiffs cannot persuasively allege that disclosure of information to USDS personnel is the same as a data breach, let alone any data breach analyzed by any federal court, or even in *New York v. Trump*, which characterizes USDS's actions as a "disclosure." 767 F. Supp. 3d 44 (S.D.N.Y. 2025), *opinion modified on denial of reconsideration*, 778 F. Supp. 3d 578 (S.D.N.Y. 2025), and *modified*, 784 F. Supp. 3d 619 (S.D.N.Y. 2025).

Turning to the Privacy Act's proximate causation requirement, Plaintiffs argue that Defendant agencies' actions were the proximate cause of the harms because "the D.C. Circuit held that allegations that the Government's actions 'opened the door to hackers, giving them ready access to a storehouse of personally identifiable and sensitive financial information' were sufficient to demonstrate proximate cause." Pls.' Resp. at 29 (quoting *In re OPM*, 928 F.3d at 67). And because in *In re OPM* the D.C. Circuit further held that "[t]he proof is in the pudding: Numerous Arnold Plaintiffs suffered forms of identity theft accomplishable only with the type of information that OPM stored and the hackers accessed." 928 F.3d at 67. Plaintiffs again conveniently leave out one critical difference. Indeed, as the D.C. Circuit made clear in that case, plaintiff "must plausibly allege that the OPM hack was the 'proximate cause' of their damages." *Id.* (citation omitted). Here, there is no hack. And there have been no plausible allegations that Defendant agencies' actions are the "proximate cause" of their claims to harm.

The remainder of their claims are difficult to reconcile. Plaintiffs again mischaracterize Defendants statements when they say that information disclosed on the dark web, along with fraudulent credit card purchases are not "hypothesized future harm[s]" as "Defendants try to claim." Pls.' Resp. at 30. But Defendants did not designate *those* alleged injuries as "hypothesized future harms." Instead, Defendants pointed to paragraphs in Plaintiffs' own Complaint stating, among other things, that permitting access to PSI puts Plaintiffs "at real risk, making them vulnerable to fraud, cyber-attack, and actual theft." Am. Compl. ¶ 79. And that, "[p]ermitting access to protected information also puts Plaintiffs . . . at great personal risk." *Id.* ¶ 80. Those are the "hypothesized future harms" that Defendants rightfully identify as not rising to a pecuniary or economic harm required to state a claim under the Privacy Act.

Plaintiffs also reject Defendants' reliance on *Keown*, finding that the plaintiffs there did not allege any specific monetary harm. Pls.' Resp. at 31. This is correct. For the simple reason that *Keown* is not a Privacy Act case (and as Defendant likewise took care to explain, Def.'s Mot. at 24-25). Plaintiffs also state that *Keown* is not on point as the court there held that the claims of

increased risk of misuse of their PSI was nevertheless sufficient to find standing for one of the plaintiffs. But this familiarly overlooks the detail that in *Keown*, there was an actual data breach from a cyberattack, and also because that case did not arise under the Privacy Act, the plaintiff that did have standing did not need to plead pecuniary harm.

***Credit & Debit Card Purchases*:** Moving to the allegations of pecuniary harm originating from the unauthorized credit and debit card purchases, Plaintiffs claim that "[t]he sequence of events alleged by the Plaintiffs creates an 'obvious inference' that the criminals who misused Plaintiffs' data obtained it from Defendants' violations of the Privacy Act." Pls.' Resp. at 32 (citation omitted). Plaintiffs cite *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 374 (1st Cir. 2023), to stand for the proposition that the temporal connection between the identity theft and the data breach was more than circumstantial. Defendants continue to highlight that the *Webb* case involved an actual data breach, again, unlike here, rendering plaintiffs' claims in *Webb* at the very least plausible.

Last, Plaintiffs argue that the secondary effect of identity theft, such as lost time spent addressing the fraudulent charges, cancelling and obtaining new cards, and the other efforts expended constitute "actual damages." 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. 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*, 578 F. Supp. 3d at 23-24 (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. Supp. 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*

OPM, 928 F.3d at 65-66 (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).

That said, in *In re OPM*, the Court there did find that one plaintiff who had spent more than 100 hours to resolve fraudulent tax return filings sufficed. 928 F.3d at 66. But the court did expressly note that regarding the Federal Rule of Civil Procedure's requirement that "special damages" be "specifically stated[,]" that "[w]e have not yet addressed whether Rule 9(g)'s heightened pleading standard applies to Privacy Act claims, and we have no occasion to do so here." *Id.* (quoting Fed. R. Civ. P. 9(g)). The Court here should find that because Plaintiffs have not "specifically stated" such pecuniary harm in this case coming from lost time and efforts, that those claims do not qualify as "pecuniary harm" under the Privacy Act's strictures. In any event, the facts in *In re OPM* are distinguishable as no Plaintiff here alleges any time and effort lost resembling that of the plaintiff who had spent more than 100 hours addressing the data breach in that case.

CONCLUSION

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

Dated: September 25, 2025

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General
Civil Division

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/ Pierce J. Anon
PIERCE J. ANON
(N.Y. Bar No. 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