IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DENISE NEMETH-GREENLEAF, JASON JUDKINS, JON MICHEL, DONNA NEMETH, AND MICHAEL RIFER, on behalf of themselves and all others similarly situated, Plaintiffs, v. UNITED STATES OFFICE OF PERSONNEL MANAGEMENT; UNITED STATES DEPARTMENT OF THE TREASURY. Defendants.	Case No. 1:25-cv-00407 Judge: Hon. Christopher R. Cooper

PLAINTIFFS' OPPOSITION TO DEFENDANTS'
MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND 3

III. LEGAL STANDARD 7

IV. ARGUMENT 7

A. Plaintiffs Have Standing Under Article III of the U.S. Constitution 7

1. Plaintiffs Suffered an Injury-In-Fact 8

a. Plaintiffs Sufficiently Allege Concrete Harms 9

b. Plaintiffs' Alleged Harms Are Based on an Invasion of a Legally Protected Interest 13

c. Plaintiffs' Alleged Harms Are Actual or Imminent 16

2. Plaintiffs' Harms Are Traceable to Defendants' Misconduct 21

B. Plaintiffs Sufficiently Allege Their Privacy Act Claim 26

1. Plaintiffs Have Sufficiently Alleged Monetary Harm in the Form of the Cost of Identity Theft Protection 27

2. Fraudulent Charges and Demonstrated Identity Theft Constitute Further Actual Damages Cognizable Under the Privacy Act 31

C. The Court Has Already Stayed the Class Certification Deadline 34

V. CONCLUSION 35

TABLE OF AUTHORITIES

Cases

All. for Retired Ams. v. Bessent, 770 F. Supp. 3d 79 (D.D.C. 2025) 13, 14, 16, 18

Allison v. Aetna, Inc., 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010) 21

Am. Fed'n of Lab. & Cong. of Indus. Organizations v. Dep't of Lab., 778 F. Supp. 3d 56 (D.D.C. 2025) 7, 14, 23

Am. Ins. Ass'n v. Selby, 624 F. Supp. 267 (D.D.C. 1985) 9

Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009) 21

Antman v. Uber Techs., Inc., 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015) 24

Arthur J. Gallagher Data Breach Litig., 631 F. Supp. 3d 573 (N.D. Ill. 2022) 12, 28, 34

Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) 8, 17

Avini Health Corp. v. Biogenus LLC, 2023 WL 2560844 (S.D. Fla. Mar. 17, 2023) 26

Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) 21

Bowen v. Paxton Media Grp., LLC, 2022 WL 4110319 (W.D. Ky. Sept. 8, 2022) 12

Carpenters Indus. Council v. Zinke, 854 F.3d 1 (D.C. Cir. 2017) 9

Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) 17, 23, 31

Comm. on Judiciary of U.S. House of Representatives v. McGahn, 968 F.3d 755 (D.C. Cir. 2020) 7

De Medicis v. Ally Bank, 2022 WL 3043669 (S.D.N.Y. Aug. 2, 2022) 23

Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018) 28

Doe v. Chao, 540 U.S. 614 (2004) 14

Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247 (11th Cir. 2021) 17

Fernandez v. Leidos, Inc., 127 F. Supp. 3d 1078 (E.D. Cal. 2015) 24

Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735 (W.D.N.Y. 2017) 25

Fus v. CafePress, Inc., 2020 WL 7027653 (N.D. Ill. Nov. 30, 2020) 24

Gadelhak v. AT&T Servs., Inc., 950 F.3d 458 (7th Cir. 2020) 15

Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) 24

Gerlich v. U.S. Dep't of Just., 659 F. Supp. 2d 1 (D.D.C. 2009) 12

Hamberger v. Eastman, 106 N.H. 107 (1964) 15

Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307 (S.D.N.Y. June 25, 2010) 21

Humane Soc'y of the U.S. v. Vilsack, 797 F.3d 4 (D.C. Cir. 2015) 7

Hummel v. Teijin Auto. Techs., v. 1 Inc., 2023 WL 6149059 (E.D. Mich. Sept. 20, 2023) 13

Hutton v. National Bd. of Examiners in Optometry, Inc., 892 F.3d 613 (4th Cir. 2018) 28

In re Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018) 25

Jeffries v. Volume Servs. Am., Inc. 928 F.3d 1059 (D.C. Cir. 2019) 15

Kassman v. American Univ., 546 F.2d 1029 (D.C. Cir. 1976) 34

Keown v. Int'l Ass'n of Sheet Metal Air Rail Transp. Workers, 2024 WL 4239936 (D.D.C. Sept. 19, 2024) 31

Kim v. McDonald's USA, LLC, 2022 WL 4482826 (N.D. Ill. Sept. 27, 2022) 23

Kylie S. v. Pearson PLC, 475 F. Supp. 3d 841 (N.D. Ill. 2020) 23

Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016) 25

Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020) 17

McGowan v. CORE Cashless, LLC, 2023 WL 8600561 (W.D. Pa. Oct. 17, 2023) 24

McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810 (E.D. Ky. 2019) 13

Mednax Services, Inc. Customer Data Sec. Breach Litig., 603 F. Supp. 3d 1183 (S.D. Fla. 2022) 17, 25

MSP Recovery, LLC v. Progressive Select Ins. Co., 2015 WL 10457208 (S.D. Fla. May 18, 2015) 25

N. Va. Hemp & Agric., LLC v. Virginia, 125 F.4th 472 (4th Cir. 2025) 9

New York Republican State Comm. v. Sec. & Exch. Comm'n, 927 F.3d 499 (D.C. Cir. 2019) 9

Newman v. Total Quality Logistics, LLC, 2021 WL 1192669 (S.D. Ohio Mar. 30, 2021) 13

Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014)..... 24

Solara Med. Supplies, LLC Customer Breach Litig., 613 F. Supp. 3d 1284 (S.D. Cal. 2020)..... 13

Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) 8, 14

Stewart v. Kendall, 578 F. Supp. 3d 18 (D.D.C. 2022) 30

Susan B. Anthony List v. Driehaus, 573 U.S. 149 (2014)..... 9

Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014) 26

TransUnion LLC v. Ramirez, 594 U.S. 413 n.7 (2021) 12

U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42 (D.C. Cir. 2019)..... passim

Uber Techs., Inc., Data Sec. Breach Litig., 2019 WL 6522843 (C.D. Cal. Aug. 19, 2019) 24

Vtech Data Breach Litig., No. 150-10889, 2017 WL 2880102 (N.D. Ill. July 5, 2017) 24

Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365 (1st Cir. 2023)..... 32

Wilding v. DNC Servs. Corp., 941 F.3d 1116 (11th Cir. 2019)..... 21

Wright v. Eugene & Agnes E. Meyer Found., 68 F.4th 612 (D.C. Cir. 2023) 7

I. INTRODUCTION

This lawsuit is brought to remedy "the largest data breach and the largest IT security breach in our country's history." First Amended Complaint ("Amended Complaint" or "FAC"), Dkt. 19. Namely, Defendants are responsible for the unauthorized disclosure of millions of federal employees' personal information. Defendants' failure to protect government employees' privacy is one of the biggest breaches of American trust by political actors since Watergate. As such, Plaintiffs bring this lawsuit to protect their privacy and to uphold the rule of law.

Millions of federal employees entrust their personal and confidential information, which includes social security numbers, dates of birth, and home addresses to the federal government as a condition of their employment, with the expectation that this data will be securely maintained. This data is collected and maintained by various governmental agencies, all of whom have a statutory duty pursuant to the Privacy Act of 1974 ("Privacy Act") to protect that personal and confidential information from improper disclosure and misuse.

Instead of steadfastly upholding that crucial duty, Defendants granted hackers access to protected data by freely providing Elon Musk and individuals within the Department of Government Efficiency ("DOGE") unfettered, unlawful access to Plaintiffs' data. Yet, Defendants now file their Motion to Dismiss, Dkt. 22 ("Mot.), in an attempt to get off scot-free, arguing that Plaintiffs lack standing and failed to state claims upon which relief may be granted, in direct contravention of clear D.C. Circuit authority. As Plaintiffs alleged in their Amended Complaint, they have already experienced actual harm as a result of Defendants' breach, including the actual misuse of their PSI, emotional distress, and time and costs spent to mitigate that harm. For example, Plaintiff Denise Nemeth-Greenleaf alleged that an identity thief made a fraudulent purchase using her Lighthouse Credit Union debit card—a card that is associated with the same credit union account information which was in Defendants' possession at the time DOGE

improperly accessed her information, as it is where Plaintiff Nemeth-Greenleaf receives her direct deposit paycheck. FAC ¶ 85. Plaintiff Donna Nemeth also alleges that two fraudulent purchases were made using a Citi Visa credit card in her name. *Id.* ¶ 84. And Defendants' misconduct cost all Plaintiffs time and money. FAC ¶¶ 14-18.

Further, Plaintiffs face imminent risk of further future harm, including identity theft, cyber-attack, and fraud. The harms wrought on Plaintiffs by Defendants dovetail with signs of government-wide exposure of Plaintiffs' and others' confidential information to unauthorized persons, including criminals, which government insiders and whistleblowers have brought to light. *See, e.g.,* FAC ¶ 49; *id.* ¶¶ 50-71 (attempts to access secured National Labor Relations Board secure systems from Russian IP address and "spike in data leaving the agency"); *id.* ¶ 72 (compromise by "unauthorized user" to Department of Treasury's Office of the Comptroller of the Currency email system); *id.* ¶ 74 (installation of Starlink transceivers at General Services Administration, including wires snaking into administrative window likely "for the purpose of siphoning off agency data."); *id.* ¶¶ 41-42 (identifying potential misuse of Department of Education employees' personal and confidential information). It was also reported that login credentials belonging to one of DOGE's own team members (who also worked at the Cybersecurity and Infrastructure Security Agency) "appeared in public leaks from info-stealer malware, **a strong indication that his devices have recently been hacked**." *Id.* ¶ 75 (emphasis added). Indeed, Plaintiff Rifer's email address, specifically one that had been on file with USAID and used by the government to communicate with him, has already been disclosed on the dark web. *Id.* ¶¶ 5, 82. The same has also happened to Plaintiff Nemeth. *Id.* ¶ 85.

Despite this lawsuit (and other related lawsuits), widespread reporting, and public outcry, Defendants have not taken steps to comply with the law and security best practices, let alone

provided relief directly to Plaintiffs for their harms. Plaintiffs, on behalf of themselves and the proposed class, aim to right these wrongs. In the meantime, Plaintiffs and millions of other federal employees past and present must face the reality that their PSI is in the hands of Elon Musk, DOGE, and likely beyond. Given the imminent and actual harm caused by Defendants' actions, and for the reasons stated below, Plaintiffs have standing to assert and have stated claims for relief under the Privacy Act. Defendants' Motion to Dismiss should therefore be denied.

II. BACKGROUND

Plaintiffs Denise Nemeth-Greenleaf, Jason Judkins, Jon Michel, Donna Nemeth, and Michael Rifer, individually and on behalf of a proposed nationwide class, bring this action for actual and statutory damages against Defendant United States Office of Personnel Management ("OPM") and Defendant United States Department of the Treasury ("Treasury Department") (collectively, "Defendants" or the "Government"), for Defendants' unlawful ongoing, systemic, and continuous disclosure of personal, health, and financial information. More specifically, the unlawfully disclosed records contained personally identifiable information including employees' full name, address, Social Security Number, driver's license, or U.S. Passport Number ("PII"), personal health information including disability status, health insurance provider information, and other medical records ("PHI"), and personal financial information including payroll, direct deposit, and financial account numbers ("PFI") (collectively, "Personal Sensitive Information" or "PSI"). In this lawsuit, Plaintiffs seek relief for Defendants' unlawful disclosure of this vast trove of protected information to non-governmental employee and private citizen Elon Musk, as well as other non-governmental employee members of the "task force" associated with the so-called "Department of Government Efficiency" ("DOGE"), and to any other unauthorized person to whom such information was disclosed.

Put another way, this lawsuit asserts violations of the Privacy Act stemming from "the

largest data breach and the largest IT security breach in our country's history." FAC ¶ 1 (quoting Charlie Warzel and Ian Bogost, THE ATLANTIC, "The Government's Computing Experts Say They Are Terrified," (Feb. 7, 2025)). Although Defendants' Privacy Act violations—and the appalling context surrounding those violations—are alleged in great detail in the First Amended Complaint, the allegations most pertinent to Defendants' Motion to Dismiss are summarized below.

Plaintiffs Denise Nemeth-Greenleaf, Jason Judkins, Jon Michel, Donna Nemeth, and Michael Rifer are just five of the millions of federal employees who "entrust their PSI to the federal government as a condition of their employment, with the expectation that this data will be securely maintained." FAC ¶¶ 2-3. OPM and the Treasury Department are executive agencies of the United States who have a statutory duty to maintain and protect information covered by the Privacy Act that is entrusted to them by Plaintiffs and their coworkers. *Id*.

Defendants have "not only failed to safeguard [the data protected by the Privacy Act]," they have "in fact willfully and intentionally permitted [protected data] to be accessed by individuals outside the United States government without legal justification and in violation of the Privacy Act." *Id*. ¶ 4. Specifically, on January 20, 2025, the day of President Donald Trump's inauguration, a presidential executive order purported to establish the "Department of Governmental Efficiency," headed by Elon Musk, who was not a federal employee in any capacity. *Id.* ¶¶ 26-27. Defendants then immediately began disclosing large swathes of PSI maintained at OPM and the Treasury Department to DOGE agents, including "individuals without a lawful or legitimate need for such data and without their having undergone the security clearance process." *Id.* ¶¶ 26, 28.

For example, in January 2025, Defendants gave Marko Elez—who was not, at the time, a government employee with the proper security clearance or training to access such data—direct

access to the Treasury Department's systems responsible for nearly all payments by the United States. *Id.* ¶ 30. Likewise, Defendants allowed at least six non-governmental employees "unfettered and unlawful administrative access" to PSI at OPM. *Id.* ¶ 33. Notably, Defendants gave unlawful access to protected records to a person allegedly fired from a prior job for having "leaked internal information to competitors" and another who "ran a company that provided support to a cybercrime gang that has bragged about trafficking in stolen data." *Id.* ¶ 34.

As Defendants acknowledge, Plaintiffs allege that OPM and the Treasury Department impermissibly disclosed the sensitive information contained in employees' "electronic Official Personnel Folder" and in the records of the Treasury Department's Bureau of Fiscal Services. *See* Mot. at 16; FAC ¶¶ 13, 20-24, 26, 29. In addition, Plaintiffs allege that Defendants unlawfully allowed non-governmental employees unfettered access to other OPM systems including "USAJOBS; USA Staffing; USA Performance; and Health Insurance (which houses information about the Federal Employee Health Benefits (FEHB) program and the Postal Service Health Benefit (PHSB) program[])]." FAC ¶¶ 32-33.

Defendants also acknowledge that Plaintiffs allege that the data exposed by Defendants' unprecedented breach of federal government systems includes—at the very least least—the "full names, addresses, social security number, driver's license, passport number, personal health information, medical records, and financial account information" for the millions of individuals currently or formerly employed by the United States. *See* Mot. at 15-16; *see also* FAC at ¶¶ 2, 20, 22-23. However, Plaintiffs also allege the Defendants' breach resulted in the unlawful disclosure of other protected data, including:

- copies of federal employees' birth certificates, documents identifying their Social Security numbers and birth dates, personal biographical information, disability status and health insurance program enrollment information, 401(k) enrollment information, personnel action investigations, character and fitness investigations,

- information collected during "background checks and security clearance investigations," including "passport information, residency details, fingerprints, and records pertaining to employees' psychological and emotional health and finances.

FAC ¶¶ 22-23.

Plaintiffs further allege that, because of Defendants' unlawful breaches, Plaintiffs have suffered or are at imminent risk of suffering from several categories of specific and actual harms that are readily traceable to Defendants' violations of the Privacy Act. These alleged harms include "(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 costs 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." Mot. at 16-17 (citing FAC ¶ 87).

In addition to alleging these more general categories of harm inflicted on them by Defendants' unlawful disclosures, Plaintiffs have asserted numerous specific examples of harm they have experienced. For example, Plaintiff Michael Rifer was notified on May 27, 2025, that his personal email address, which was on file with the Government, was found on the "dark web" along with a strong possibility of other sensitive information being breached as well. *Id.* ¶ 83. In addition, Plaintiff Donna Nemeth learned that two fraudulent purchases were made on April 2 and April 16, 2025, on a card in her name. *Id.* ¶ 84. Similarly, fraudulent purchases were made using a debit card in the name of Plaintiff Denise Nemeth-Greenleaf, made only days apart on April 4 and April 15, 2025; the account for this card was on file with the Government as it was used for direct deposit payments. *Id.* ¶ 85. Similarly, as with Plaintiff Rifer, Plaintiff Nemeth-Greenleaf's

email address, used by the Government for communications with her, was recently discovered on the dark web. *Id*. Further, and significantly, Plaintiffs have each alleged that they purchased identity theft monitoring and/or protection services in direct response to Defendants' actions. *See* FAC ¶¶ 14-18; *see also id*. ¶ 81 (Plaintiffs "reasonably fear harmful consequences of the disclosure and use of their PSI").

III. LEGAL STANDARD

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) for lack of Article III standing, Plaintiffs' "complaint must state a plausible claim" of standing. *Humane Soc'y of the U.S. v. Vilsack*, 797 F.3d 4, 8 (D.C. Cir. 2015); *Am. Fed'n of Lab. & Cong. of Indus. Organizations v. Dep't of Lab.*, 778 F. Supp. 3d 56, 69 (D.D.C. 2025) ("*AFL*") (citing same). In assessing allegations of standing, courts must "accept facts alleged in the complaint as true and draw all reasonable inferences from those facts in the plaintiffs' favor." *Humane Soc'y of the U.S.*, 797 F.3d at 8. Importantly, while assessing whether plaintiffs have standing, "the [C]ourt must assume that [they] will prevail on the merits" of their legal claims. *Comm. on Judiciary of U.S. House of Representatives v. McGahn*, 968 F.3d 755, 762 (D.C. Cir. 2020).

To defeat a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted, a complaint "must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Wright v. Eugene & Agnes E. Meyer Found.*, 68 F.4th 612, 619 (D.C. Cir. 2023). The Court "must treat the complaint's factual allegations as true, and must grant [the] plaintiff the benefit of all inferences that can be derived from the facts alleged." *Id*.

IV. ARGUMENT

A. Plaintiffs Have Standing Under Article III of the U.S. Constitution

In their Motion, Defendants first seek dismissal under Rule 12(b)(1), contending this Court

does not have subject matter jurisdiction over Plaintiffs' claims because Plaintiffs lack Article III standing. Under Article III of the U.S. Constitution, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). In their Motion to Dismiss, Defendants only challenge "injury-in-fact" and "traceability" and do not dispute that Plaintiffs satisfy the redressability requirement.[1]

Plaintiffs' Amended Complaint alleges multiple injuries that provide a basis to "clear[ ] the low bar to establish their standing at the pleading stage." *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 622 (D.C. Cir. 2017). Moreover, certain aspects of Defendants' standing challenge go directly to the merits of Plaintiffs' claims, and therefore are not appropriate for resolution at the motion to dismiss stage. This Court should therefore deny Defendants' Motion to Dismiss under Rule 12(b)(1).

1. Plaintiffs Suffered an Injury-In-Fact

To establish the injury-in-fact element of the Article III standing inquiry, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339. An injury is particularized if it "affect[s] the plaintiff in a personal and individual way." *Id*. An injury is concrete when it is "real," not "abstract." *Id*. at 352. Importantly, intangible injuries like the threat of future injury may be concrete. *Id*. at 339. "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a "'substantial risk" that the harm will

[1] Nor could Defendants plausibly dispute redressability. Plaintiffs' harms would plainly be redressed by class treatment, an award of actual and statutory damages, including prejudgment interest, an award of costs and disbursements assessed by Plaintiffs in connection with this action, including reasonable attorneys' fees, and an award of any other relief this Court deems just and proper. FAC ¶¶ 33-32.

occur.'" *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). The injury need not be substantial: "an identifiable trifle will suffice." *Am. Ins. Ass'n v. Selby*, 624 F. Supp. 267, 270 (D.D.C. 1985) (citation omitted); *see also New York Republican State Comm. v. Sec. & Exch. Comm'n*, 927 F.3d 499, 504 (D.C. Cir. 2019) ("As we have long held, even a slight injury is sufficient to confer standing[.]"); *Carpenters Indus. Council v. Zinke*, 854 F.3d 1, 5 (D.C. Cir. 2017) (collecting cases). As demonstrated below, Plaintiffs' injuries here are concrete, based on invasion of a legally protected interest, and actual or imminent.

a. Plaintiffs Sufficiently Allege Concrete Harms

Plaintiffs sufficiently allege several concrete harms as a result of Defendants' "unlawful ongoing, systemic and continued disclosure of [Plaintiffs'] personal, health, and financial information," FAC ¶ 2, including actual misuse of their PSI, time and costs incurred in mitigating harm from the continuing breach of their PSI, an imminent risk of identity theft in the future, a loss of privacy and confidentiality of their PSI, and emotional distress.[2] Each of these harms have been upheld by courts as sufficient to confer standing.

***Actual Misuse*:** Plaintiffs allege actual misuse of their PSI, which is sufficient to confer standing. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 55 (D.C. Cir. 2019) ("As we have already recognized, 'identity theft constitute[s] a concrete and particularized

[2] Defendants confusingly argue that Plaintiffs do not have standing based on harms suffered by their family members, but the FAC is almost exclusively focused on harms suffered by Plaintiffs themselves. Indeed, the allegation quoted by Defendants states that Plaintiffs were harmed because they cannot avoid having "PSI **for themselves** and their family members maintained in government records. . ." Mot. at 20 (citing FAC ¶ 77) (emphasis added). The scant other references to Plaintiffs' family members in the Amended Complaint similarly appear in conjunction with reference to Plaintiffs. While Defendants themselves acknowledge that harm to family members as a result from government action **can** give rise to standing, that is not the basis of Plaintiffs' standing here. *Id.* (citing *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 489 (4th Cir. 2025). Plaintiffs reserve all rights to further amend their Complaint should a family member incur such injury that would further confer standing.

injury.'" (quoting *Attias*, 865 F.3d at 627); *see also Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (offering the "increased risk of fraud or identity theft" as an "example" of a "concrete consequence" for standing purposes). Here, Plaintiff Denise Nemeth-Greenleaf alleged that an identity thief made a fraudulent purchase using her Lighthouse Credit Union debit card that is associated with the same credit union account information in Defendants' possession at the time DOGE improperly accessed her information. FAC ¶ 85. Plaintiff Donna Nemeth also alleges two fraudulent purchases were made using a Citi Visa credit card in Plaintiff Nemeth's name. *Id.* ¶ 84.

Imminent Risk of Identity Theft: Plaintiffs likewise allege that Defendants' loosening of access control to Plaintiffs' PSI, especially where it permitted DOGE to "easily find individuals in databases or clone entire servers and transfer that secure information somewhere else," *id.* ¶ 37, presents a significant risk of identity theft because "[s]uch access and disclosure to persons without proper vetting or training makes Plaintiffs' and Class Members' PSI more vulnerable to hacking, identity theft, and other malicious activity by foreign adversaries or other malignant actors." *Id.* ¶ 38.

Providing important context, Plaintiffs' Amended Complaint details the dire consequences of OPM's last data breach, where the PSI of federal employees was compromised by foreign adversary actors, *id.* ¶ 47. Given that background and the value of Plaintiffs' PSI to hackers and bad actors, an expert opined that DOGE's access to this information is "a field day" for hackers "with a bunch of college kids running around with sensitive federal government data." *Id.* ¶ 48; *see also id.* ¶ 74. Indeed, soon after Defendants unlawfully provided individuals associated with DOGE access to Plaintiffs' PSI, at least two Plaintiffs reported that they received notifications that some of the same PSI that was in Defendants' possession is now on the dark web. *See id.* ¶¶ 5, 82

(Plaintiff Rifer received a notification that his email address on file with USAID and used by the government to communicate with him has been disclosed on the dark web, and that his other personal information may be compromised); *id.* ¶ 5 (Plaintiff Nemeth-Greenleaf received notification that her email address on file with the Department of the Navy has been disclosed on the dark web).

Likewise, the Amended Complaint is replete with allegations that some agencies have already reported data irregularities and potential misuse of the same since DOGE improperly accessed their records systems. *See e.g.*, FAC ¶ 49; *id.* ¶¶ 50-71 (attempts to access secured National Labor Relations Board secure systems from Russian IP address and "spike in data leaving the agency"); *id.* ¶ 72 (compromise by "unauthorized user" to Department of Treasury's Office of the Comptroller of the Currency email system); *id.* ¶ 74 (installation of Starlink transceivers at General Services Administration, including wires snaking into administrative window likely "for the purpose of siphoning off agency data."); *id.* ¶¶ 41-42 (identifying potential misuse of Department of Education employees' PSI). It was reported that login credentials belonging to one of DOGE's own team members (who also worked at the Cybersecurity and Infrastructure Security Agency) "appeared in public leaks from info-stealer malware, **a strong indication that his devices have recently been hacked**." *Id.* ¶ 75 (emphasis supplied). Thus, to the extent that Plaintiffs' PSI was available on his devices, that information is likely in the hands of a malicious actor.

As discussed *infra* § IV.A.2, since the filing of Plaintiffs' FAC, the Social Security Administration's former Chief Data Officer filed a whistleblower complaint detailing how DOGE members uploaded a copy of a critical Social Security database that included "records of all Social Security numbers issued by the federal government . . . individuals' full names, addresses and birth dates, among other details that could be used to steal their identities, making it **one of the nation's**

most sensitive repositories of personal information[,]" in June to a "vulnerable cloud server, putting the personal information of hundreds of millions of Americans at risk of being hacked or leaked."[3][4] Each of these instances of mishandling Plaintiffs' and class members' PSI underscores the likelihood that their information will be misused in the future, and because Defendants have refused to remedy DOGE's unauthorized access as alleged in Plaintiffs' Amended Complaint, the imminent risks of identity theft Plaintiffs face will continue in the future. FAC ¶ 86.

Emotional distress: Allegations of fear and anxiety resulting from an unlawful disclosure of PSI, like those alleged by Plaintiffs, have been upheld by courts as sufficient to confer standing. *See, e.g.*, *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 n.7 (2021) ("a plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm."); *In re. Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 587 (N.D. Ill. 2022) (allegations of anxiety and increased concern for the loss of privacy from a data breach sufficed as legally cognizable injuries); *Bowen v. Paxton Media Grp., LLC*, 2022 WL 4110319, at *6 (W.D. Ky. Sept. 8, 2022) (averments of mental distress related to plaintiffs' fear of identity theft and of stress, nuisance and annoyance of dealing with issues resulting from a data breach as sufficient to show cognizable injury). Here, Plaintiffs allege that they have suffered emotional distress as a result of the breach and that they "reasonably fear harmful consequences of the disclosure and use of their PSI." *See* FAC ¶ 81; *see also id.* ¶ 87.

Time spent and costs to mitigate harm from Defendants' breach: Courts routinely recognize that time spent dealing with instances of actual fraud and attempting to mitigate future

[3] *See* Nicholas Nehamas, DOGE Put Critical Social Security Data at Risk, Whistle Blower Says, *N.Y. Times*, (Aug. 26, 2025), available at archive.is/7gsTw (emphasis added).

[4] "A court may consider material other than the allegations of the complaint in determining whether it has jurisdiction to hear the case, so long as it still accepts the factual allegations in the complaint as true." *Gerlich v. U.S. Dep't of Just.*, 659 F. Supp. 2d 1 (D.D.C. 2009) (cleaned up).

damages are recognized are concrete injuries that support Article III standing. *See Hummel v. Teijin Auto. Techs., v. 1 Inc.*, 2023 WL 6149059, at *11-12 (E.D. Mich. Sept. 20, 2023) (noting the "host of alleged damages" including lost time resulting from a data breach); *Newman v. Total Quality Logistics, LLC*, 2021 WL 1192669, at *4 (S.D. Ohio Mar. 30, 2021) (recognizing mitigation costs to prevent misuse of stolen data is injury); *In re Solara Med. Supplies, LLC Customer Breach Litig.*, 613 F. Supp. 3d 1284, 1296 (S.D. Cal. 2020) (noting that "time spent monitoring one's credit and other tasks associated with responding to a data breach" is an injury); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019). Here, Plaintiffs Nemeth-Greenleaf, Judkins, Michel, Nemeth, and Rifer have each purchased some kind of credit and/or identity theft monitoring to try to mitigate the plainly foreseeable harms that are impending—and indeed now already occurring—as a result of Defendants' failure to comply with the Privacy Act. FAC ¶¶ 14-18, 114(d). Plaintiffs likewise allege that they have been damaged in the form of "lost opportunity costs associated with effort expanded and the loss of productivity from addressing and attempting to mitigate any consequences . . . including but not limited to efforts spent researching how to prevent, detect, contest and recover from data misuse." *Id.* ¶ 114(d); *see also id.* ¶ 114(g).

b. Plaintiffs' Alleged Harms Are Based on an Invasion of a Legally Protected Interest

Plaintiffs have suffered actual and imminent injuries similar to those that have been upheld by courts in this district examining the same conduct under the Privacy Act against the same or similar defendants. Defendants' argument to the contrary, that Plaintiffs' claims are not based on the invasion of a legally protected interest, largely relies on a concurrence by Judge Richardson in the Fourth Circuit's opinion in *Am. Fed'n of Tchrs. v. Bessent*, where Judge Richardson argued that the harm from a Privacy Act violation is not close enough to the tort of intrusion upon seclusion. *See* 2025 WL 1023638, at *4 (4th Cir. Apr. 7, 2025). Defendants do not rely on **any**

cases from this District; indeed, the only reference to cases in this District is a footnote that acknowledges that this District's courts reached the opposite conclusion "that the plaintiffs have standing to pursue their Privacy Act claims in similar (though not identical) circumstances." Mot. at 9, n.2 (citing *AFL*, 778 F. Supp. 3d 56; *All. for Retired Ams. v. Bessent*, 770 F. Supp. 3d 79 (D.D.C. 2025)).[5] Defendants identify no reason to diverge from this precedent and otherwise make no attempt to distinguish it, nor could they.

Indeed, in *AFL*, this District considered the exact same concurrence Defendants rely on and expressly disagreed with it.[6] This District recognized, as set forth in *TransUnion*:

> "[I]n determining whether a harm is sufficiently concrete to qualify as an injury in fact, . . . Congress's views may be 'instructive.'" [TransUnion, 594. U.S. at 426] (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). . . . Congress can "'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).

AFL, 778 F. Supp. 3d at 72 (parallel citations omitted). The court went on to analyze the statutory purpose of the Privacy Act, which is to "protect the privacy of individuals identified in information systems maintained by Federal Agencies[,]" *id.* (citing *Doe v. Chao*, 540 U.S. 614, 618 (2004)

---

[5] The sentence following Defendants' acknowledgement of this Court's favorable-to-Plaintiffs precedent appears to be incomplete. *See* Mot. at 9, n.2. To the extent Defendants intended to imply that *Soc. Sec. Admin. v. Am. Fed'n of State, Cnty. & Mun. Emps.,* 145 S. Ct. 1626 (2025) ("*SSA*") warrants discarding this District's precedent, they are mistaken. In *SSA*, the Supreme Court merely recited the factors it considers in determining whether to grant a stay of a preliminary injunction and stated that the stay should be granted without analyzing the factors or offering any analysis. *Id.* At a maximum, all that can be gleaned from *SSA* is that the Supreme Court had some concern about the preliminary injunction at issue, but here Plaintiffs are not seeking an injunction. In any event, these circumstances have clearly changed given the recent SSA whistleblower action about DOGE's dangerous practices vis-à-vis SSA's data. *See supra* § IV.A.2 regarding actual/imminent harm.

[6] Defendants also rely briefly on Judge Agee's concurrence in *Am. Fed'n of Tchrs.*, though as the court in *AFL* explained, that concurrence applies nonbinding precedent examining the Telephone Consumer Protection Act ("TCPA"), while Judge Richardson's concurrence examines the Privacy Act. *AFL*, 778 F. Supp. 3d at 71. Apart from the *Am. Fed'n of Tchrs.* concurrences, Defendants similarly rely on inapt TCPA cases. *See* Mot. at 10.

(quoting The Privacy Act)), while restricting that information to only "those employees with a need to view it," *id*. This, the court explained, represents an identification by Congress of an interest that is "a modern relative of a harm with long common law roots." *Id.* (quoting *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.)). The *AFL* court reasoned that this effectively created a new sphere of seclusion for those who are protected by the Privacy Act, and "an intrusion upon that sphere—even if the sphere literally encompasses only one row of millions in a dataset—**amounts to an injury similar to the intrusion upon other private spheres, such as one's home**." *Id.* (emphasis added) (citing *Hamberger v. Eastman*, 106 N.H. 107, 110–112 (1964) ("The tort of intrusion upon the plaintiff's solitude or seclusion is not limited to a physical invasion of his home or his room or his quarters," but rather extends "beyond such physical intrusion" and includes "eavesdropping upon private conversations by means of wire tapping and microphones." (internal quotation marks omitted)).

In addition to intrusion upon seclusion, the *AFL* court noted this Circuit has "recognized that the tort of 'breach of confidence' can serve as a common-law analogue for a harm inflicted by a statutory violation" which arises "where a person offers private information to a third party in confidence and the third party reveals that information to another." *Id.* at 73 (citing *Jeffries v. Volume Servs. Am., Inc.* 928 F.3d 1059, 1064 (D.C. Cir. 2019)); *see also All. For Retired Americans*, 770 F. Supp. 3d at 104 ("Even if Defendants could show that an invasion of Plaintiffs' members' privacy interests in the information stored in the Treasury's systems of records would not be actionable at common law, that invasion would still implicate the same *kind* of harm that common law courts recognize.") (punctuation and citation omitted, alteration in the original). The *AFL* court concluded that because the plaintiff organizations allege "their members gave DOL and HHS their personal information in confidence, backed by the Privacy Act's guarantee that the

agencies would not disclose the information to any other person or agency . . . **their members are currently suffering actionable harm for the sole reason that the agency defendants are disclosing the plaintiffs' members' personal information to unauthorized individuals**." *Id.* at 73 (emphasis added); *see also All. For Retired Americans*, 770 F. Supp. at 104 ("[T]he injury that Plaintiffs allege that their members face is a concrete injury-in-fact for Article III purposes.").

Plaintiffs here have demonstrated that they, too, are suffering actionable harm because of Defendants' violation of the Privacy Act and disclosure of their personal information to unauthorized individuals. Thus, this Court should follow this District's precedent and reach the same conclusion here.

c. Plaintiffs' Alleged Harms Are Actual or Imminent

Defendants next argue Plaintiffs' alleged harms are speculative. Mot. at 13-17.[7] As discussed above, Plaintiffs have plausibly alleged actual harms. *See supra* § IV.A.1.a. (detailing allegations of actual misuse, emotional distress, and time spent and costs to mitigate Defendants' breach). Defendants take special issue with Plaintiffs' allegations that Defendants' misconduct puts Plaintiffs at imminent risk of "fraud, cyber-attack, and actual theft." FAC ¶ 79; *see also supra* § IV.A.1.a. (discussing same); *id*. (discussing past data breach of OPM and multiple data irregularities and potential misuse of the same since DOGE has accessed it, as described by insiders and experts). Specifically, Defendants argue that Plaintiffs' allegations regarding this risk rely on a "highly attenuated chain of possibilities." Mot. at 14. Not so.

First, Plaintiffs do not need to be "literally certain" that their data will be misused, at least

[7] It is difficult to parse Defendants' standing arguments regarding whether Plaintiffs' harms are concrete, actual or imminent, and traceable to Defendants' disclosure of their PSI. Defendants' arguments as to all three boils down to the following: there is no impact to Plaintiffs from Defendants' disclosure of their PSI. Dkt. 15-17. Plaintiffs' arguments in response apply equally to Defendants' standing arguments to the extent they overlap.

at this stage. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 415 n.5 (2013).

Second, the harms already experienced by Plaintiffs support their allegations that DOGE and other unauthorized actors have and will continue to misuse their PSI, thereby exposing them to substantial risk of identity theft and fraud. FAC ¶¶ 37, 50, 82-86. Indeed, where, as here, some Plaintiffs have alleged actual misuse of their PSI, such allegations alone are sufficient to substantiate a risk of future harm on all the named Plaintiffs. *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021) ("Beyond the sufficient risk of identity theft and resulting injuries, a vast number of Plaintiffs who have not yet suffered identity theft also allege they have spent time, money, and effort mitigating the risk of identity theft. . . . [B]ecause the risk of harm here is a sufficient injury, the allegations of mitigation injuries made by these Plaintiffs are also sufficient."); *see also In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D. Md. 2020) (explaining that plaintiffs who did not allege actual misuse of their PII adequately pled imminent threat of identity theft because "the allegations about the targeting of personal information in the cyberattack and the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent");[8] *In re Mednax Services, Inc. Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1202 (S.D. Fla. 2022) (recognizing plaintiffs' allegations of actual misuse are "helpful in

[8] In *Marriott*, the data that was compromised included only PII—such as names, mailing addresses, phone numbers, email addresses, passport numbers, and dates of birth. *Id.* at 460-61. Notably, it did not include social security numbers, or PHI and PFI like the data at issue here does, underscoring the severity of any potential compromise to Plaintiffs' PSI. Indeed, the D.C. Circuit has recognized that other types of information, including but not limited to, dates of birth, driver's license numbers, and health insurance information, can also be extremely valuable to thieves. *See Attias*, 865 F.3d at 628 (reversing the district court's order dismissing the action for lack of standing, observing that plaintiffs whose health insurance information was compromised in a data breach alleged "at the very least, a plausible allegation that [they] face a substantial risk of identity fraud, even if their social security numbers were never exposed to the data thief").

establishing a 'substantial risk' of future harm for plaintiffs who remain unaffected").

Third, Plaintiffs' allegations are akin to those in *AFL*, 778 F. Supp. 3d at 69-70, where this District recognized plaintiffs' "suffering because DOL and HHS have unlawfully given [DOGE] personnel access to agency systems that contain the members' PII (giving rise to both their APA and Privacy Act claims)." The court held such harm was "imminent" where plaintiffs alleged "[Defendant] DOL leadership directed agency employees to give [DOGE] personnel access to 'any DOL system,' . . . and that HHS has granted USDS personnel access to CMS and other HHS systems." *Id*. at 70. So too here. *See* FAC ¶ 26 (Defendants gave access to people without lawful or legitimate need or security clearances), ¶ 29 (detailing same as to DOT leadership), ¶ 31 (same as to OPM), ¶¶ 32-35. As such, "[i]t takes no chain of speculation to conclude from these allegations that [Defendants] are providing [DOGE] personnel access to systems that contain plaintiffs' [PSI]." *AFL*, 778 F. Supp. at 70.[9]

Fourth, that Plaintiffs' allegations regarding these risks are plausible is further supported by events that have occurred since the filing of Plaintiffs' Amended Complaint. [10] Indeed, the Social Security Administration's former Chief Data Officer filed a whistleblower complaint detailing how DOGE members uploaded a copy of a critical Social Security database that included "records of all Social Security numbers issued by the federal government . . . individuals' full

[9] For this reason, Defendants' conclusory citations on this point are inapposite. *See Murthy v. Missouri*, 603 U.S. 43, 70 (2024) (finding no standing where a theory of injury "rel[ies] on a speculative chain of possibilities"); *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 77 (D.D.C. 2016) (finding no standing where the likelihood that plaintiff will suffer further harms remains "entirely speculative…"). Further, unlike in *Laird v. Tatum*, where there was no dispute about whether the disclosure was for a "valid government purpose," here Plaintiffs' allegations are that Defendants had **no** valid government purpose and, at a minimum, that fact is in dispute. *See* 408 U.S. 5, 10-11 (1972).

[10] "A court may consider material other than the allegations of the complaint in determining whether it has jurisdiction to hear the case, so long as it still accepts the factual allegations in the complaint as true." *Gerlich*, 659 F. Supp. 2d at 1 (cleaned up).

names, addresses and birth dates, among other details that could be used to steal their identities, making it **one of the nation's most sensitive repositories of personal information**[,]" in June of 2025 to a "vulnerable cloud server, putting the personal information of hundreds of millions of Americans at risk of being hacked or leaked."[11] This buttresses Plaintiffs' allegations of risk of future misuse, and, because Defendants have refused to remedy DOGE's unauthorized access as alleged in Plaintiffs' Amended Complaint, the imminent risks of fraud, cyber-attack, and actual theft Plaintiffs face will only continue. FAC ¶ 86; *see also In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d at 54–55 ("[G]iven [ ] Plaintiffs' allegations regarding OPM's continued failure to adequately secure its databases, it is reasonable to infer that there remains a 'substantial risk' that their personal information will be stolen from OPM again in the future.").

The cases Defendants cite for their proposition that these risks to Plaintiffs are merely "conjectural" or "hypothetical" are either inapplicable here or actually support Plaintiffs' claims. For example, *Doe v. Off. of Pers. Mgmt.*, 2025 WL 513268 (D.D.C. Feb. 17, 2025), is inapposite because it did not involve a Privacy Act claim or any improper disclosure, but rather a claim under the E-Government Act of 2002 based on OPM's failure to conduct an adequate Privacy Impact Assessment where the only associated risk alleged was to government email addresses on file. Defendants' citation to *Univ. of Cal. Student Ass'n v. Carter*, 766 F. Supp. 3d 114, 121-122 (D.D.C. 2025), in support of their standing argument is similarly, at minimum, puzzling and, at worst, dubious. The *Carter* court expressly declined to rule on standing, holding only that the motion for a temporary restraining order was denied because plaintiffs had not met the D.C. Circuit's "high standard for [showing that] irreparable injury" would result if unrestrained.

[11] *See* Nicholas Nehamas, DOGE Put Critical Social Security Data at Risk, Whistle Blower Says, *N.Y. Times*, (Aug. 26, 2025), archive.is/7gsTw (emphasis added).

Critically, in declining to rule on the standing questions, the court stated "[t]hose questions are **less clear cut and are better answered on a more complete record**." *Id*. at 121 (emphasis added). This last point is in Plaintiffs' favor, as it counsels that Plaintiffs are entitled to discovery, not dismissal.

Neither does *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. Soc. Sec. Admin.*, 771 F. Supp. 3d 717, 771 (D. Md. 2025) ("*AFL-CIO*"), help Defendants. There, the court expressly distinguished its holding finding no standing from that in *New York v. Trump*, 767 F.Supp.3d 44 (S.D.N.Y. 2025), where standing was satisfied on the basis that plaintiffs in the *New York* case alleged:

> [T]he Treasury DOGE Team was mistakenly granted read/write permissions instead of read-only permission…The critical sensitivity of the information contained in the Bureau of the Fiscal Service payment systems, which includes the PII and confidential information of both the States and millions of their residents, requires more than a band-aid approach to cybersecurity.

AFL-CIO, 771 F. Supp. 3d at 771.

Here, Plaintiffs' allegations are akin to those in the *New York* case, where the court found standing satisfied and therefore distinct from those in *AFL-CIO*, 771 F. Supp. 3d at 771. *See* FAC ¶ 37 ("[E]ven with 'read only' access to Plaintiffs' PSI—which Plaintiffs do not concede is the highest level of access Defendants have so far provided to unauthorized users, as reports indicate that certain individuals, including Elez, were also provided with 'write' access[ ]—'Musk's people could easily find individuals in databases or clone entire servers and transfer that secure information somewhere else.").[12] The other out-of-circuit cases Defendants cite in conclusory

[12] FAC ¶ 37 cites Victoria Elliott, Leah Feiger, and Tim Marchman, WIRED, "The US Treasury Claimed DOGE Technologist Didn't Have 'Write Access' When He Actually Did" (Feb. 6, 2025), perma.cc/A8T4-E9Q6.

fashion are also inapposite. Mot. at 15.[13]

Finally, it is worth emphasizing that Plaintiffs' allegations are not speculative merely because they have not yet **proven** that DOGE and others have "read Plaintiffs' individual data," as Defendants suggest. Mot. at 26 (though Plaintiffs plausibly allege that their PSI **was** read and misused). Obtaining such proof is the very purpose of discovery, so Plaintiffs do what they must at this stage: plausibly allege their harms are actual and imminent. *See infra* § IV.A.2 (discussing how courts resolve fact-intensive standing questions at the merits stage).

2. Plaintiffs' Harms Are Traceable to Defendants' Misconduct

Contrary to Defendants' arguments, Mot. at 17, Plaintiffs amply allege their harms are traceable to Defendants' misconduct. "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be fairly traceable' to the defendant." *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d at 54 (citing *Attia*, 865 F.3d at 629). "[E]ven harms that flow indirectly from the action in question can be said to be 'fairly traceable' to that action for standing purposes" *Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1125 (11th Cir. 2019).

Plaintiffs' allegations plainly meet this permissive standard. Plaintiffs allege their PSI was

[13] *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), concerned only "names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight)," unlike here, and the court ruled on standing **after** "extensive discovery." The court in *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010), also decided standing **at summary judgment** after plaintiffs failed to "adduce[ ] any evidence in discovery" of risk of harm. In *Allison v. Aetna, Inc.*, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010), the breach "did not contain Plaintiff's banking, financial, or health information" but rather "some email addresses which [hackers allegedly] then used in an attempt to elicit personal information via spam" and "Defendant offered Plaintiff credit monitoring assistance and identity theft insurance," unlike here. In *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009), plaintiff "appear[ed] to concede [ ] there has been no publication of any information allegedly wrongfully obtained, nor any fraudulent or otherwise harmful use of such information[,]" unlike here.

disclosed as a result of Defendants' misconduct. *See, e.g.*, FAC ¶ 26 ("Beginning shortly after the inauguration of President Donald Trump on January 20, 2025, Defendants OPM and Treasury Department illegally and improperly violated these restrictions on disclosure of PSI by giving access to that PSI to individuals without a lawful or legitimate need for such data and without their having undergone the security clearance process."). And Plaintiffs explain how Defendants' disclosure of their PSI has resulted in harms to Plaintiffs, including actual misuse, *id*. ¶¶ 84-85, imminent risk of identity theft, *id.* ¶¶ 41-42, 47-48, 50-72, 74-75, emotional distress, *id.* ¶¶ 81, 87, and time and money spent to mitigate harms from Defendants' breach, *id.* ¶¶ 14-18, 114(d). Taken as true with all reasonable inferences construed in Plaintiffs' favor, these allegations plausibly establish a link between Defendants' misconduct and Plaintiffs' harm.[14]

Defendants wrongly urge this Court to adopt a traceability standard that is both too strict for this stage in the proceedings, and also conflates the merits of Plaintiffs' case with standing. Defendants claim Plaintiffs fail to allege "any public disclosure or data breach of their PSI beyond mere speculation." Mot. at 18. This ignores Plaintiffs' plain, well-pled allegations. To be sure, Plaintiffs allege that by providing unauthorized individuals access to Plaintiffs' PSI, Defendants thereby **disclosed** it, the underlying facts of which are undisputed. *See* FAC ¶ 26 (alleging Defendants provided access to PSI to "individuals without a lawful or legitimate need for such data and without their having undergone the security clearance process."). Defendants also contradict Plaintiffs' allegations that these disclosures to unauthorized persons exposed Plaintiffs' PSI to third-party bad actors (as supported by allegations of the harms already experienced by

[14] Defendants' only attack the link between their conduct and **some** of Plaintiffs' alleged harms, taking aim solely at Plaintiffs' allegations of actual misuse and imminent risk of identity theft, and leaving Plaintiffs' allegations regarding the connection between Defendants' conduct and their other harms unrebutted, including Plaintiffs' allegations regarding (a) the time and money spent to mitigate harms from Defendants' breach, and (b) their related emotional distress.

Plaintiffs Rifer, Nemeth, and Nemeth-Greenleaf), and to substantial risk of future harm as to all Plaintiffs. *See supra* §§ IV.A.1.a and A.1.b. "It takes no chain of speculation to conclude from these allegations that [Defendants] are providing [DOGE] personnel access to systems that contain plaintiffs' members' [PSI]." *Am. Fed'n of Lab. & Cong. of Indus. Organizations*, 778 F. Supp. at 56 (citing *Clapper*, 568 U.S. at 411–14).

Defendants also improperly characterize Plaintiffs' factual allegations as to traceability by arguing, without support, that the PSI at issue is so "innocuous" that, even if disclosed, it could not be used to harm Plaintiffs. Mot. at 30-31. This ignores the incredibly broad range of PSI that was in Defendants' possession and to which Defendants provided unauthorized access, which included information more than sufficient for bad actors to cause Plaintiffs harm. *See* FAC ¶ 20 (Defendant Treasury Department disclosed "names, Social Security numbers, birth dates, and bank account information."); *id.* ¶¶ 22-24 (Defendant OPM disclosed, *inter alia*, "employees' birth certificates, documents identifying their Social Security numbers and birth dates, personal biographical information, disability status and health insurance program enrollment information, 401(k) enrollment information, personnel action investigations, character and fitness investigations;" "passport information, residency details, fingerprints, and records pertaining to employees' psychological and emotional health and finances;" and "federal applicants' records including PSI, background investigations, and security clearance forms."). In this way, Defendants' disclosures included far more—and constitute far worse breaches—than mere "publicly available" information.[15] Indeed, the PSI at issue here is closer to, though in combination

[15] For the same reason, Defendants' cases on this point do not help them. *See Kim v. McDonald's USA, LLC*, 2022 WL 4482826, at *5 (N.D. Ill. Sept. 27, 2022) (concerning "non-sensitive email addresses, phone numbers, and delivery addresses"); *Kylie S. v. Pearson PLC*, 475 F. Supp. 3d 841, 848 (N.D. Ill. 2020) (concerning names, emails, and birthdays); *De Medicis v. Ally Bank*, 2022 WL 3043669, at *10 (S.D.N.Y. Aug. 2, 2022) (concerning only editable username and

still more sensitive than, the information at issue in *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 386 (6th Cir. 2016), which held that plaintiffs had standing to bring data breach claims when the breached database contained personal information such as "names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers.". *See* Mot. at 20 (citing *Galaria*).

Regarding the named Plaintiffs, Defendants only explicitly attack Plaintiffs Rifer, Nemeth, and Nemeth-Greenleaf, claiming they cannot link their allegations of identity theft and fraud to Defendants' actions, Dkt. 29 (citing *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 32 (D.D.C. 2014)).[16] Again, Plaintiffs need not **prove** such a link at the pleading stage. Even so, Plaintiffs plausibly allege such a link. *See infra* § IV.A.2. Unlike in *SAIC*, where "[n]o one allege[d] that credit-card, debit-card, or bank-account information was on the stolen tapes," here Plaintiffs allege that the sensitive information that bad actors have and can continue to use at Plaintiffs' expense **was** in the files Defendants disclosed to unauthorized persons and thereby exposed more broadly. *See id*.; *see also* FAC ¶¶ 20, 22-24 (identifying range of PSI in Defendants' possession and disclosed).[17] And Plaintiffs provide examples of how Defendants'

---

password); *Fus v. CafePress, Inc.*, 2020 WL 7027653, at *3 (N.D. Ill. Nov. 30, 2020) (concerning "billing and shipping address and personal email address"); *In re Vtech Data Breach Litig.*, No. 150-10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) ("[D]ata stolen here did not include credit-card or debit-card information…"); *McGowan v. CORE Cashless, LLC*, 2023 WL 8600561 at *1, *11 (W.D. Pa. Oct. 17, 2023), *report and recommendation adopted*, 2024 WL 488318 (W.D. Pa. Feb. 8, 2024) (concerning "names, addresses, email addresses, phone numbers, and payment card information"); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019) (concerning "basic contact information and driver's license"); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (concerning no "social security numbers, account numbers, or credit card numbers").

[16] As 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.

[17] Defendants' citation to *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015)—which itself cites and relies on *SAIC*, 45 F. Supp. 3d at 31—is similarly inapposite.

disclosure of their combined PSI has led to harms already. *See, e.g.*, FAC ¶ 83 (Plaintiff Rifer's personal email address on file with the Government was found on the "dark web"); *id.* ¶ 85 (Fraudulent purchases were on a debit card in the name of Plaintiff Nemeth-Greenleaf, the account for which was on file with the Government as it was used for direct deposit payments). This is in line with the D.C. Circuit's holding in *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*:

> [E]ven if the breaches in question did not expose all information necessary to make fraudulent charges on victims' existing financial accounts, the personal data the hackers did manage to obtain is enough, by itself, to enable several forms of identity theft. That fact, combined with the allegations that at least some of the stolen information was actually misused after the breaches, suffices to support a reasonable inference that [ ] Plaintiffs' risk of future identity theft is traceable to the OPM cyberattacks. Neither the likelihood that some [ ] Plaintiffs experienced other types of unrelated fraud nor the speculative possibility that they might also have been the victims of other data breaches renders causation implausible here.

928 F.3d at 60; *see also In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) ("[T]hat some other [actor] *might* also have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue for the breach in question.") (cleaned up). So too here.

Finally, in the alternative, even if Defendants' arguments regarding traceability held water (which they do not), 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. *See, e.g.*, *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 757, 758 (W.D.N.Y. 2017) (collecting cases); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 969 (7th Cir. 2016) (holding that whether "fraudulent charges can[ ] be attributed to its data breach" is "a theory of defense that P.F. Chang's will be entitled to pursue at the merits phase."); *In re Mednax Services, Inc. Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1202 (S.D. Fla. 2022) (finding it "prudent to deny the motion [to dismiss]" because defendants' standing arguments were "indirect, if not direct, attacks on the merits" of plaintiffs' claims); *MSP Recovery, LLC v. Progressive Select Ins. Co.*, 2015 WL 10457208, at *2 (S.D. Fla. May 18, 2015) ("[T]he Court finds that it is prudent to address

the standing issue at the summary judgment stage, where the Court may consider the entire factual record that the parties have developed during the course of discovery."); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding defendant's standing arguments "gloss over the actual allegations made and set a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage."); *Avini Health Corp. v. Biogenus LLC*, 2023 WL 2560844, at *3 (S.D. Fla. Mar. 17, 2023) (denying the motion to dismiss because the factual challenges to plaintiff's standing were "nothing more than a denial of the allegations in the [complaint] and the Court will not resolve this dispute until the parties have had a full opportunity to conduct discovery.").

B. Plaintiffs Sufficiently Allege Their Privacy Act Claim[18]

Defendants argue that Plaintiffs' claims must be dismissed because Plaintiffs failed to assert actual damages resulting from the Privacy Act violations. Mot. at 32. As demonstrated below, this is false and ignores the plausible allegations set forth in Plaintiffs' Amended Complaint.

As an initial matter, Defendants either misunderstand the damages Plaintiffs seek through this action or are misrepresenting those damages in its Motion before the Court. As requested in the Amended Complaint, Plaintiffs seek the recovery of monetary damages. Dkt. 19, ¶¶ 114 (seeking "actual damages and pecuniary losses"), Prayer for Relief (seeking "actual and statutory

[18] Defendants puzzlingly move to dismiss Plaintiffs' Federal Information Security Modernization Act ("FISMA") claim (Mot. at 30-31), but the FAC does not allege a FISMA cause of action, so there is nothing to dismiss. Rather, Plaintiffs reference FISMA among several rules and regulations focused on maintaining appropriate information security, which Defendants disregarded in the course of violating the Privacy Act. Defendants' request to dismiss Plaintiffs' non-existent FISMA cause of action has no bearing on Plaintiffs' FISMA-related allegations, which support that Defendants failed to comply with basic information security policies and procedures, and does not provide justification to dismiss any part of this action.

damages"). To the extent other, non-monetary, harms are discussed, they are intended to further demonstrate the severity and effect of the Government's violations.[19] Accepting the facts as set forth in the Amended Complaint as true, which this Court must, Plaintiffs have more than sufficiently alleged that they have suffered monetary harm as a result of the Defendants' actions, a harm which can be redressed through this litigation. Specifically, among other things, Plaintiffs have suffered the monetary loss associated with the costs of purchasing identity theft protection and actual losses as a result of credit card identity theft. *Id.* ¶¶ 14-18, 84-85. Thus, Defendants' Motion must be denied.

1. Plaintiffs Have Sufficiently Alleged Monetary Harm in the Form of the Cost of Identity Theft Protection

Defendants make two faulty arguments in support of their argument that Plaintiffs have not alleged monetary harm. First, Defendants argue that Plaintiffs have failed to assert any pecuniary harm resulting from the Defendants' Privacy Act violations because the costs of purchasing identity theft protection services are "self-imposed mitigation costs." Mot. at 34. Defendants further claim that not only do such costs generally do not qualify as pecuniary harm but that they specifically do not qualify here because there is allegedly no substantial risk of future harm to be mitigated. *Id.* This is false on both counts, particularly in light of controlling D.C. Circuit precedent.

The D.C. Circuit has held, in no uncertain terms, that the costs of credit protection and/or credit repair services following a data breach "**are the paradigmatic example of 'actual**

[19] Defendants identify a single instance in which Plaintiffs mention "injunctive relief" in their Amended Complaint. Mot. at 41 (citing FAC ¶ 2). This sole reference to injunctive relief is a clerical error, as Plaintiffs have otherwise removed their request for injunctive relief from all other parts of the Amended Complaint, including, most notably, the Prayer for Relief. Compare Dkt. 1 (Original Complaint) to Dkt. 19 (FAC). To be clear, Plaintiffs are not seeking injunctive relief in this matter.

damages' resulting from the violation of privacy protections." *U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.,* 928 F.3d at 65 (emphasis added). Indeed, in so holding, the Circuit Court reversed the district court's grant of the Government's motion to dismiss on this exact ground. *Id.* This holding is consistent with other appellate courts. *See also Dieffenbach v. Barnes & Noble, Inc.,* 887 F.3d 826, 830 (7th Cir. 2018) (overturning district court grant of a motion to dismiss, finding allegations of monthly cost of credit monitoring services following disclosure of personal information by a merchant is a form of "actual damage" sufficient to demonstrate compensable damages); *Hutton v. National Bd. of Examiners in Optometry, Inc.,* 892 F.3d 613, 622 (4th Cir. 2018) ("costs of mitigating measures to safeguard against future identify theft" in the form of purchasing credit monitoring services, where substantial risk of harm actually exists, is sufficient to demonstrate an injury-in-fact). Here, Defendants' strained attempt to claim that *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.* is somehow distinguishable from this case because in that earlier case, allegedly unlike here, there was "an actual data breach" should be disregarded, 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**. FAC ¶¶ 26-40. There is no reason to treat the instant situation differently from *U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig*.

In addition, the Amended Complaint alleges that Plaintiffs' damages were proximately caused by the Defendants' Privacy Act violation, which is sufficient to allege "actual damages" for purposes of the Privacy Act. As this Circuit has explained, such a showing requires the Plaintiffs to plausibly allege that the Defendants' conduct was a "substantial factor in the sequence of events leading to [] Plaintiffs' injuries, and those injuries must have been reasonably foreseeable or anticipated as a natural consequence of" the Defendants' conduct. *Id.* at 67. Notably, "[t]o be

the proximate cause is not necessarily to be the sole cause." *Id.*

Here, Plaintiffs have specifically alleged that their personal and confidential protected information, which was maintained by the Defendants in their capacity as Plaintiffs' employer, was unlawfully shared with numerous unauthorized individuals in violation of the Privacy Act. FAC ¶¶ 26-40. Such information included, among other things, federal employees' birth certifications, documents identifying their Social Security numbers and birth dates, personal biographical information, disability status and health insurance program enrollment information, 401(k) enrollment information, personnel action investigations, character and fitness investigations, passport information, residency details, fingerprints, and records pertaining to employees' psychological health and finances. *Id.* ¶¶ 22-23. Plaintiffs further allege that, upon learning of the unauthorized disclosure of their personal information, they took specific steps to secure their personal information and protect their identity by purchasing identity theft and/or credit monitoring protections. *Id.* ¶¶ 14-18.

Notably, in *U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 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. *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.,* 928 F.3d at 67. The 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." *Id.*

The same is true here. Plaintiffs have made specific allegations that the Defendants' unlawful disclosures reflect actual identity theft as well as heightened Plaintiffs' risk of identity theft, and that the exact personal, confidential, and protected information Defendants stored and

maintained has appeared on the dark web and has been compromised through fraudulent credit card purchases not long after Defendants opened the door to hackers. FAC ¶¶ 83-85. This is not "hypothesized future harm" (Mot. at 34) as Defendants try to claim. Instead, there has already been actual theft and further disclosure of the personal information unlawfully disclosed by Defendants. Moreover, as discussed above, Amended Complaint includes citations to publicly reported expert opinions providing that the disclosures which occurred here have thrown open the gates to cybersecurity intrusions by foreign adversaries and has greatly increased the risk of data exposure. *See, e.g.*, FAC ¶¶ 48, 54, 68-69, 74. In addition, the FAC details that there have already been at least two known instances of access to Government systems and employee personnel information by outside intruders—both at the National Labor Relations Board and the Office of the Comptroller of the Currency.[20] *Id.* ¶ 48-75.

These facts are clearly sufficient to demonstrate, particularly at this early stage, that there is a real and substantial risk of future harm resulting from the Defendants' Privacy Act violations. Thus, to the extent Defendants rely on *Stewart v. Kendall* to argue that Plaintiffs' claims must be dismissed, such reliance is misplaced. *See* Mot. at 33. Indeed, in *Stewart*, the court held that "mitigation costs incurred to prevent future injury **can qualify as actual damages** . . . if there is at least a substantial risk of future harm." *Stewart,* 578 F. Supp. 3d 18, 25 (D.D.C. 2022) (finding no injury-in-fact based on mitigation efforts where plaintiff "does not allege he is at a substantial risk of future identity theft or other damages because of the breach," and distinguishing Stewart's

[20] Indeed, on August 26, 2025, The New York Times reported that, per a whistleblower complaint, DOGE team members (the same team members who Plaintiffs have alleged engaged in Privacy Act violations here) uploaded a Social Security database containing personal information of hundreds of millions of Americans, including full names, birth dates, and Social Security numbers, to a vulnerable cloud server and which put such data at risk of being compromised. Nicholas Nehamas, "DOGE Put Critical Social Security Data at Risk, Whistle-Blower Says," THE NEW YORK TIMES (Aug. 26, 2025), available at archive.is/7gsTw.

circumstances from cases in which a substantial risk of future harm was found based on a data breach where the plaintiffs' personal information had already been accessed) (emphasis added).[21] Defendants' reliance on *Keown*, Mot. at 36, is similarly inapposite, as the *Keown* plaintiffs did not allege any specific monetary harm—only that they had experienced a heightened risk of misuse of personal information and lost time spent on mitigation measures. *See Keown v. Int'l Ass'n of Sheet Metal Air Rail Transp. Workers,* 2024 WL 4239936, at *9-10 (D.D.C. Sept. 19, 2024). Moreover, the *Keown* court held that this was nevertheless sufficient to support the plaintiff's negligence claims and demonstrate actual injury at the motion to dismiss stage because his allegations relating to mitigation efforts resulted from knowledge that his PII was disseminated on the dark web and that he experienced an increase in spam calls, texts, and/or emails. *See id*.

Accordingly, because Plaintiffs have alleged "actual damages" in the form of pecuniary loss resulting from their purchase of identity theft protection and credit monitoring services, purchases that were made precisely **because of** Defendants' unauthorized disclosures in violation of the Privacy Act, Defendants' motion to dismiss must be denied.

2. Fraudulent Charges and Demonstrated Identity Theft Constitute Further Actual Damages Cognizable Under the Privacy Act

Defendants' arguments for dismissal based on the Plaintiffs' allegations of fraudulent credit card charges and actual identity theft fair no better than their assertions with respect to the costs of identity theft and credit monitoring and protection. As the Amended Complaint makes

[21] The instant case is also distinguishable from *Clapper v. Amnesty Intern. USA,* 568 U.S. 398 (2013), repeatedly cited by Defendants. *Clapper* involved the issue of standing under the Foreign Intelligence Surveillance Act (FISA) and did not involve any Privacy Act claims. Further, the *Clapper* court held that "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 417. But, here, as described above, there is no "hypothetical future harm that is not certainly impending"—there is **actual harm** resulting from Defendants' Privacy Act violations as well as a real, and serious, risk of substantial future harm.

clear, Plaintiffs allege that Defendants' Privacy Act violations have already resulted in multiple, specific instances of actual harm to Plaintiffs, including the identity theft that immediately followed Defendants' unlawful disclosures of Plaintiffs' PSI.

Defendants' first argument on this point—that Plaintiffs failed to plausibly allege a causal connection between the data breach and the fraudulent charges on financial accounts that were included in the breached data and that occurred immediately following the breach—is meritless on its face. The 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. *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 374 (1st Cir. 2023) (rejecting a similar argument in a defendant's motion to dismiss, noting the "obvious temporal connection" between the identity theft and the data breach). It is no "logical leap," as Defendants claim, for Plaintiffs to allege a causal connection between the sudden instances of identity theft occurring within 90 days of the Privacy Act violations underlying this lawsuit.

Further, Defendants' claim that the "fraudster had no way to make the alleged unauthorized charges with just the information provided to Defendant agencies," Mot. at 39, misconstrues Plaintiffs' allegations. Plaintiffs have alleged that far more sensitive PSI than only the "name, account number, and routing number," Mot. at 38, for Plaintiff Nemeth-Greenleaf's bank account have been exposed by Defendants' unlawful conduct. Rather, Defendants' violations of the Privacy Act have exposed, **at least**, their "full name, address, Social Security Number, driver's license or U.S. Passport Number, . . . disability status, health insurance provider information, . . . payroll, direct deposit, and financial account numbers," FAC ¶ 2, "birth dates, personal biographical information, disability status and health insurance program enrollment information, 401(k) enrollment information, personnel action investigations, character and fitness

investigations," *id*. ¶ 20, "passport information, residency details, fingerprints, and records pertaining to employees' psychological and emotional health and finances," *id*. ¶ 22, among a great deal more. To suggest that an identity thief could not make use of the unbelievably broad scope of data exposed by Defendants' unlawful actions to access Plaintiffs' financial accounts defies simple common sense. Here, where the Court must "assume the truth of all plaintiffs' plausibly pleaded allegations, and draw all reasonable inferences in their favor," *Agnew v. District of Columbia*, 920 F.3d 49, 53 (D.C. Cir. 2019), Defendants' artificially narrowed account of events cannot be credited.

Defendants' second argument—that identity theft and fraudulent charges do not constitute "actual damages" for purposes of the Privacy Act—is directly foreclosed by controlling D.C. Circuit caselaw, as discussed above. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d at 65. As the D.C. Circuit has explained, it would be error to conclude that allegations of fraudulent transactions do not state a claim for actual harm under the Privacy Act simply because there is no allegation they are unreimbursed. As the Circuit explicitly held when rejecting a similar argument from the Government concerning fraudulent loans and purchases made in plaintiffs' names: "Those financial losses qualify as 'actual damages.'" *Id.* (citing *Federal Aviation Admin. v. Cooper*, 566 U.S. 284, 298–299 (2012)). "At this stage of the litigation, all facts and reasonable inferences must be drawn in favor of the [Plaintiffs], and the complaint provides no basis for disregarding the claimed financial losses based on [Defendants'] speculation that [Plaintiffs] were indemnified." *Id*.

Moreover, even if Plaintiffs are fully indemnified against losses from fraudulent charges, the "collateral source" doctrine also forecloses Defendants' argument for dismissal. As the D.C. Circuit has explained, even fraudulent charges that were fully reimbursed support a claim under

the Privacy Act because "an injured person may usually recover in full from a wrongdoer regardless of anything he may get from a collateral source unconnected with the wrongdoer." *Id.* (quoting *Kassman v. American Univ.*, 546 F.2d 1029, 1034 (D.C. Cir. 1976) (per curium)). In other words, Defendants' speculation about the extent that the harm dealt to Plaintiffs has been mitigated by a third party—whether mistaken or not—provides no basis to dismiss Plaintiffs' claims.

Finally, even setting aside the actual, direct costs of identity theft, courts have also recognized that "actual damages" can include the secondary effects of identity theft, such as lost time spent addressing the fraudulent charges, canceling and obtaining new cards, difficulties in making purchases with cards flagged for possible fraud, and similar issues. *See, e.g.*, *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 587–88 (N.D. Ill. 2022) (finding fraudulent charges leading to plaintiff being "unable to purchase furniture" constituted pecuniary harm under a related state law); *In re: Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *6 (D. Minn. June 2, 2022) (notifications of credit card fraud and time spent mitigating the damage constituted actual, concrete, and particularized injury, under related state law). Thus, Plaintiffs' allegations are sufficient to give rise to an inference of these additional secondary effects that result in actual damages to the Plaintiffs.

This Court should reject Defendants' arguments that the identity theft incidents suffered by Plaintiffs in the immediate aftermath of, and as a direct result of, Defendants' Privacy Act violations, do not constitute actual damages. As set forth above, Plaintiffs have alleged more than sufficient actual damages resulting from Defendants' violations of the Privacy Act.

C. The Court Has Already Stayed the Class Certification Deadline

Defendants ask the Court to resolve Defendants' Motion to Dismiss prior to class certification. Mot. at 31-32. However, this Court has already resolved this issue. On April 28, 2025, Plaintiff filed an unopposed motion, requesting the Court to "enter an order holding the class

certification deadline in abeyance pending entry of a scheduling order." Dkt. 16 at 2. On April 29, 2025, the Court granted Plaintiff's motion, holding the deadline for class certification in abeyance. Dkt. 17. Plaintiffs' position on the issue has not changed, so there is no need for further Court action on this particular issue.

V. CONCLUSION

Plaintiffs request that the Court deny Defendants' Motion to Dismiss in full. If, however, the Court decides to grant Defendants' Motion in any respect, Plaintiffs seek leave to amend, which should be freely given under Federal Rule of Civil Procedure 15.

Dated: September 18, 2025

Respectfully submitted,

/s/ Sara L. Faulman
Gregory McGillivary (D.C. Bar No. 411029)
Sara L. Faulman (D.C. Bar No. 496679)
John W. Stewart (D.C. Bar No. 1028836)
Sarah M. Block (D.C. Bar No. 1026577)
McGILLIVARY STEELE ELKIN LLP
1101 Vermont Ave. NW, Suite 1000
Washington, DC 20005
(202) 833-8855
gkm@mselaborlaw.com
slf@mselaborlaw.com
jws@mselaborlaw.com
smb@mselaborlaw.com

Andrea R. Gold DC (D.C. Bar No. 502607)
Hassan A. Zavareei (D.C. Bar No. 456161)
Gemma Seidita DC (D.C. Bar No. 1721862)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW, Suite 1010
Washington, DC 20006
(202) 919-5852
agold@tzlegal.com
hzavareei@tzlegal.com
gseidita@tzlegal.com

Cort T. Carlson (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
(510) 254-6808
ccarlson@tzlegal.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on September 18, 2025, I filed the foregoing document using the Court's ECF system, which causes a copy to be emailed to all counsel of record.

/s/ Sara L. Faulman
Sara L. Faulman