UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

FEDERAL DEFENDANT'S MOTION TO DISMISS
THE CONSOLIDATED AMENDED COMPLAINT

Federal Defendant, the Office of Personnel Management ("OPM"), by and through its undersigned counsel, hereby moves to dismiss Plaintiffs' Consolidated Amended Complaint in this multidistrict litigation, Case No. 1:15-mc-01394-ABJ (ECF No. 63), pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and 9(g). Accompanying this motion is a memorandum of points and authorities in support of the motion along with three exhibits. Defendant respectfully requests that the Court grant the motion for the reasons described in the memorandum.

Dated: May 13, 2016

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director, Federal Programs Branch

/s/ Matthew A. Josephson
MATTHEW A. JOSEPHSON
ANDREW E. CARMICHAEL
KIERAN G. GOSTIN
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch

20 Massachusetts Avenue, NW, Room 7304
Washington, DC 20530
Tel: (202) 514-9237
Email: Matthew.A.Josephson@usdoj.gov

Counsel for Federal Defendant OPM

CERTIFICATE OF SERVICE

I hereby certify that on May 13, 2016, I filed the above motion with the Court's CM/ECF system, which will send notice of such filing to all parties.

/s/ *Matthew A. Josephson*
Matthew A. Josephson

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF FEDERAL DEFENDANT'S MOTION TO DISMISS THE CONSOLIDATED AMENDED COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Legislative Materials

Other

PRELIMINARY STATEMENT

In June and July 2015, the Office of Personnel Management ("OPM") announced that two separate but related cyber incidents had been carried out against the United States Government, resulting in the theft of personnel records and background investigation records of current, former, and prospective federal employees and government contractors. Combined, the two cybersecurity incidents affected the sensitive information of approximately 22 million people. After the incidents, the federal government sent notices to impacted individuals and offered comprehensive identity-theft protection and credit monitoring services, at no cost to the individuals. Congress thereafter passed legislation extending these benefits to ensure at least ten years of coverage.

Plaintiffs in this multidistrict litigation case are a union representing federal employees—the American Federation of Government Employees ("AFGE")—and thirty-eight individuals who received notice that their information may have been compromised in the OPM cybersecurity incidents. Plaintiffs generally allege that OPM and its contractor, KeyPoint Government Solutions Inc. ("KeyPoint"), failed to adequately protect their personal information and that this failure led to the cyber intrusions into OPM's systems. With respect to Defendant OPM, Plaintiffs seek money damages under the Privacy Act, contractual damages under the Little Tucker Act, and expansive injunctive relief under the Administrative Procedure Act, including broad judicial oversight of OPM's information-security practices.

This entire multi-district case should be dismissed because Plaintiffs cannot establish legal standing or state a claim under the federal statutes they have identified. Many legal obstacles require dismissal of Plaintiffs' claims, but perhaps most fundamental is Plaintiffs' inability to establish actual injury or compensable loss caused by the OPM incidents. Although the thirty-eight individual Plaintiffs allege in their Complaint certain identity-theft incidents they have experienced since OPM announced that its systems were intruded, Plaintiffs do not plead any facts showing that these

disparate harms—which range from unauthorized charges on credit cards to the filing of fraudulent tax returns to the misuse of a Social Security number—are attributable to any data breach, let alone the OPM data breaches.

Plaintiffs' causal theory is dependent, not on OPM or KeyPoint's actions, but rather on the independent actions of third-party cyber intruders or other wrongdoers not before this Court. To establish that the OPM incidents are the source of the alleged harms in the Complaint, one would have to make numerous speculative assumptions, none of which are supported by factual allegations. These include assumptions that the third parties have read (or, for claims based on future injury, will read) a particular Plaintiff's information (out of a group of over 20 million), have misused (or intend to misuse) a particular category of information compromised in the OPM cybersecurity incidents, and have been (or will be) successful in misusing a particular Plaintiff's information as a result of the OPM incidents.

In addition, as we discuss throughout this motion, the issue of causation in data breach cases is significant because the harms commonly alleged (and the ones alleged here) are ubiquitous in today's digital world. Around seven percent of the adult population in the United States—over 17 million people—will experience some form of identity theft every single year. In part for this reason, scores of federal courts have dismissed data breach cases because the alleged harms are simply consistent with living in a digital society, and not plausibly traceable to a particular data breach, or even to any data breach at all, given the wealth of personal information (Social Security numbers, credit card numbers, etc.) that individuals disclose to others on a regular basis. And in the very few data-breach cases where courts have permitted the case to proceed past the pleadings, there have been allegations of widespread, systemic financial fraud immediately following the breach of a financial database storing active account information. Such allegations are not present here. The OPM incidents did not involve financial databases storing active financial account information, and

the alleged fraud following the incidents is comparatively minimal, quite disparate, and consistent with the fraud experienced by the general population.

Even if Plaintiffs had adequately pled facts that would establish standing – and they have not – the United States has not waived immunity from this suit. Plaintiffs' claims and requested remedies must fall within specific and unambiguous waivers of sovereign immunity contained in the Privacy Act, the Little Tucker Act, or the APA. These statutes only waive immunity under specific circumstances and do not provide relief here. For example, the Privacy Act requires a Plaintiff to plead personal monetary loss in order to state a claim. No Plaintiff, however, pleads facts showing that he or she has suffered monetary loss as a result of the OPM cybersecurity incidents. For this and all the other reasons discussed below, all of the claims in the Consolidated Amended Complaint should be dismissed.

BACKGROUND

I. STATUTORY BACKGROUND

A. The Privacy Act of 1974

The Privacy Act of 1974 establishes "a comprehensive and detailed set of requirements" for federal agencies that maintain systems of records containing individuals' personal information. *FAA v. Cooper*, 132 S. Ct. 1441, 1446 (2012). As relevant here, the Privacy Act prohibits a federal agency from disclosing "any record which is contained in a system of records" unless certain exceptions apply. 5 U.S.C. § 552a(b); *see also id.* § 552a(a)(4)-(5). In addition, the Act requires agencies to "establish appropriate administrative, technical, and physical safeguards" in order to keep records secure and to guard against anticipated security threats that could substantially harm, embarrass, inconvenience, or cause unfairness to an individual for whom an agency record is maintained. 5 U.S.C. § 552a(e)(10).

The Privacy Act vests the district courts with jurisdiction over any civil action brought by an individual who has been adversely affected by a violation of the Act. *See* 5 U.S.C. § 552a(g)(1)(A). The form of civil relief authorized by the Act depends on the particular violation alleged. As relevant here, the Privacy Act authorizes courts to award monetary damages when the agency fails "to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual." *Id.* § 552a(g)(1)(C)-(D), (g)(4). The "adverse effect" requirement "acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue." *Doe v. Chao*, 540 U.S. 614, 624 (2004).

To recover monetary damages, a plaintiff must do more than demonstrate standing and show that the agency failed to satisfy its Privacy Act obligations. The plaintiff must also plead and prove facts showing "that the agency acted in a manner which was intentional or willful" and that, as a result, the plaintiff suffered "actual damages." 5 U.S.C. § 552a(g)(4). "Actual damages" under the Privacy Act "are limited to actual pecuniary loss, which must be specially pleaded and proved." *See Cooper*, 132 S. Ct. at 1451, 1453. The federal government retains sovereign immunity from liability for all other kinds of injury. *Id.* at 1456.

B. The Little Tucker Act

The Little Tucker Act waives the federal government's sovereign immunity for certain money-damages claims not sounding in tort. *See United States v. Bormes,* 133 S. Ct. 12, 15 (2012). Subject to exceptions not relevant here, the Little Tucker Act provides that "district courts shall have original jurisdiction, concurrent with the United States Court of Federal Claims," of a "civil action or claim against the United States, not exceeding $10,000 in amount, founded either upon the Constitution, or any Act of Congress, or any regulation of an executive department, or upon any

express or implied contract with the United States, or for liquidated or unliquidated damages in cases not sounding in tort." 28 U.S.C. § 1346(a)(2). The Little Tucker Act and its companion statute, the Tucker Act, 28 U.S.C. § 1491(a)(1), do not themselves "creat[e] substantive rights," but "are simply jurisdictional provisions that operate to waive sovereign immunity for claims premised on other sources of law." *Bormes*, 133 S. Ct. at 16-17 (citing *United States v. Navajo Nation*, 556 U.S. 287, 290 (2009)).

C. The Administrative Procedure Act

The Administrative Procedure Act ("APA"), 5 U.S.C. §§ 701–06, establishes a waiver of sovereign immunity and a cause of action for injunctive relief for parties adversely affected either by agency action or by an agency's failure to act. *See* 5 U.S.C. § 706(1)-(2); *see also Heckler v. Chaney*, 470 U.S. 821, 828 (1985). The APA, however, has several important limitations. Section 702 declares that APA review is not available "if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought" by the plaintiff. 5 U.S.C. § 702. Section 702 accordingly "prevents plaintiffs from exploiting the APA's waiver to evade limitations on suit contained in other statutes." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2204-05 (2012). Similarly, Section 704 requires that the person seeking APA review of final agency action have "no other adequate remedy in a court," 5 U.S.C. § 704. To preclude APA review, the alternative remedy "need not provide relief identical to relief under the APA, so long as it offers relief of the same genre." *Garcia v. Vilsack*, 563 F.3d 519, 522 (D.C. Cir. 2009) (citation omitted). The APA also explicitly excludes from judicial review those agency actions that are "committed to agency discretion by law." 5 U.S.C. § 701(a)(2). Finally, while the APA allows a court to compel "agency action" that is withheld contrary to law or unreasonably delayed, § 706(1), or to set aside "agency action" under certain circumstances, § 706(2), such claims can only proceed if

a plaintiff identifies a "discrete agency action that [the agency] is required to take." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64 (2004).

D. Federal Information Security Management Act and the Federal Information Security Modernization Act

In 2002, Congress passed the Federal Information Security Management Act ("FISMA"), 44 U.S.C. §§ 3541–3549, as Title III of the E–Government Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899. In 2014, Congress updated FISMA by passing the Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, 128 Stat. 3073 (codified at 44 U.S.C. §§ 3551-3558 (2014)).[1] FISMA provides "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). Among other things, FISMA seeks to provide for "development and maintenance of minimum controls required to protect Federal information and information systems" and for "improved oversight of Federal agency information security programs." *Id.* § 3551(3)-(4). To achieve these aims, FISMA assigns the Director of the Office of Management and Budget ("OMB") the exclusive responsibility for overseeing the management and security of information systems of civilian agencies. 44 U.S.C. § 3553(a)(5); 40 U.S.C. § 11303(b)(5). FISMA also allocates a multitude of information-security responsibilities to a host of entities, including the OMB, the Department of Commerce, the Department of Homeland Security, the National Institute of Standards and Technology, the Comptroller General, the public, and multiple officials in each federal agency. *See generally* 44 U.S.C. §§ 3551–3558.

---

[1] As a result of the update to FISMA in the Modernization Act, the sections in the United States Code codifying FISMA have been renumbered. The current version of FISMA is codified at 44 U.S.C. §§ 3551-3558 (2014). For clarity, OPM has cited the current version of FISMA in the U.S. Code.

II. FACTUAL BACKGROUND AND PROCEDURAL HISTORY

A. The Cybersecurity Incidents at OPM

This case arises from two separate but related cybersecurity incidents involving the information technology systems and data managed by OPM. *See* Plaintiffs' Consolidated Amended Complaint ("CAC") ¶¶ 125-33 (ECF No. 63).[2]

In June 2015, OPM publicly announced that it had identified a cybersecurity incident affecting the personnel data of approximately 4 million current and former federal employees. CAC ¶ 138; *see also* OPM Ex. 1, OPM Announcement (June 4, 2015). OPM advised that the investigation of the incident was ongoing and that it would notify individuals whose information may have been compromised. *Id.* The data compromised in the personnel incident included an individual's name, Social Security number, birth date, place of birth, and current or former address. *See* OPM – Cybersecurity Resource Center, Cybersecurity Incidents, "What Happened," https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited May 13, 2016).

In July 2015, OPM publicly announced that it had identified a separate but related cybersecurity incident on its systems involving background investigation records. CAC ¶ 140; OPM Ex. 2, OPM Announcement (July 9, 2015). OPM explained that the background investigation records of current, former, and prospective federal employees and contractors had been stolen from

---

[2] The following factual background is taken from Plaintiffs' CAC and OPM's public announcements of the cybersecurity incidents. The public announcements are incorporated by reference in the CAC. *See* CAC ¶¶ 138-41 (referencing public announcements). They accordingly may be considered in resolving this motion to dismiss. *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 20 & n.2 (D.D.C. 2014). In addition, when a court considers jurisdictional arguments, it may rely on evidence outside of the complaint. *Id.* at 23 (citing *Jerome Stevens Pharms., Inc. v. FDA*, 402 F.3d 1249, 1253 (D.C. Cir. 2005)). For purposes of this motion to dismiss under Rule 12(b)(6), the factual allegations are accepted as true. *See*, *e.g.*, *Atherton v. Dist. of Columbia Office of the Mayor*, 567 F.3d 672, 681 (D.C. Cir. 2009).

its databases. *Id.* OPM determined that sensitive information, including the Social Security numbers of approximately 21.5 million individuals, were stolen. *Id.* The data impacted in the background-investigation incident included information submitted by applicants for federal employment in Standard Form 85, 85P, and 86. CAC ¶¶ 66-71. The affected data included Social Security numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; certain health, criminal and non-account financial history; usernames and passwords used to fill out investigation forms; and some records included findings from interviews conducted by background investigators and fingerprints. OPM Announcement (July 9, 2015), Ex. 2. Notably, while a background-investigation file could possibly contain information regarding mental health and financial history provided by a particular individual, "there is no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of federal personnel were impacted by this incident." *Id.* at 2.

Following the cybersecurity incidents, OPM outlined a series of discretionary steps it would take to protect impacted individuals. *Id.* at 2-4; CAC ¶ 148. Most notably, the federal government sent notices to individuals affected by the cybersecurity incidents, and provided a comprehensive suite of monitoring and identity-theft insurance services free of charge. CAC ¶ 148. These free-of-charge services include identity monitoring of public database sources; credit monitoring services; identity restoration services in the event a particular individual's identity is compromised for any reason, even if unrelated to the incidents; and no-deductible identity-theft insurance for any possible expenses that might be incurred in restoring one's identity.[3] Congress recently extended these benefits. In the Consolidated Appropriations Act of 2016, Congress provided the individuals

[3] A full description of the suite of services offered to individuals affected by the cybersecurity incidents is available on OPM's website (https://www.opm.gov/cybersecurity/cybersecurity-incidents/) (last visited May 13, 2016) under the tab "Supporting people who have been affected".

affected by the cybersecurity incidents with at least 10 years of comprehensive monitoring services and increased identity theft insurance coverage. *See* Pub. L. No. 114-113, § 632, 129 Stat. 2242, 2470-71 (2015).

B. Procedural Background

1. Consolidation and Coordination through the JPML Process

This multi-district litigation ("MDL") action is composed of twenty separate cases filed in numerous districts across the United States. On October 5, 2015, the U.S. Judicial Panel on Multidistrict Litigation ("JPML") granted OPM's motion to create the present case pursuant to 28 U.S.C. § 1407, transferring the extra-district actions to this District and assigning the MDL to this Court. *See* JPML Transfer Order (ECF No. 1). In November 2015, the Court entered the Initial Practice and Procedure Order, which, among other things, directed all parties in the MDL to meet and confer, submit a proposed Case Management Plan, and attend the Initial Scheduling and Case Management Conference on December 15, 2015 (ECF No. 8).

After the Case Management Conference, the Court entered a scheduling order (ECF No. 19). As pertinent here, the Court, at the request of the parties, required that a Consolidated Amended Complaint be filed for all transferred cases, except *National Treasury Employees Union v. Archuleta*, No. 15-cv-1808-ABJ (D.D.C. 2015) ("NTEU"), and that the CAC will serve as the superseding, operative complaint for all Plaintiffs in this MDL, except the NTEU Plaintiffs. Plaintiffs timely filed the CAC on March 14, 2016.[4]

[4] OPM will file a separate motion to dismiss the action *NTEU v. Archuleta*, No. 15-cv-1808-ABJ (D.D.C. 2015).

2. The Consolidated Amended Complaint

The CAC names OPM and its contactor KeyPoint as Defendants. CAC ¶¶ 51-53. Plaintiffs are AFGE and thirty-eight individuals who allege that their information was compromised in the OPM cybersecurity incidents. CAC ¶¶ 11, 13-50.[5] The CAC is brought as a putative class action on behalf of all individuals whose information was subject to the OPM cybersecurity incidents. CAC ¶¶ 164-74.

With respect to OPM, the CAC alleges four counts: Count One alleges that OPM violated the Privacy Act's safeguards provision, 5 U.S.C. § 552a(e)(10), by failing to maintain adequate safeguards to ensure the security of Plaintiffs' information. Count One further alleges that OPM violated the disclosure provision of the Act, *id.* § 552a(b), by unlawfully disclosing Plaintiffs' information. For relief, Plaintiffs seek actual and statutory damages under 5 U.S.C. § 552a(g)(1)(D) and (g)(4). *See* CAC ¶¶ 175-85.

Count Two alleges a breach of contract claim against OPM under the Little Tucker Act, 28 U.S.C. § 1346(a). Plaintiffs allege that their submission of SF-85, SF-85P, and SF-86 forms to the government created a binding contract that required the protection of the information in those forms from unauthorized disclosure, and that this contract was breached when Plaintiffs' information was stolen during the cybersecurity intrusions. For relief, Plaintiffs seek unspecified contractual damages. *See* CAC ¶¶ 186-95.

---

[5] The CAC names five Plaintiffs by the pseudonym "John Doe" or "Jane Doe." *See* CAC ¶¶ 22-26. A plaintiff may only proceed anonymously under a pseudonym in exceptional cases, and requests to proceed anonymously are rarely granted. *See*, *e.g.*, *Qualls v. Rumsfeld*, 228 F.R.D. 8, 10 (D.D.C. 2005). Plaintiffs have provided no sound basis for proceeding anonymously in this case. Nonetheless, the Court need not rule on this issue on this motion because the claims asserted by all Plaintiffs, including John and Jane Does, should be dismissed for the myriad reasons discussed below.

Count Three alleges that OPM violated the APA by failing to comply with the FISMA, the Privacy Act, and regulations and technical standards for data security issued by the Office of Management and Budget and the National Institute for Standards and Technology. Plaintiffs ask the court to set aside past agency action as arbitrary and capricious under Section 706(2)(A), and to compel OPM to comply with unspecified provisions of the FISMA (and perhaps other unspecified rules) in the future under Section 706(1). *See* CAC ¶¶ 196-207.

Count Four alleges a partially duplicative claim for declaratory and injunctive relief under the APA, the Declaratory Judgment Act, and the Court's "inherent authority to order equitable remedies." Plaintiffs seek a declaration that OPM's past conduct was unlawful; indemnification for any future injury sustained by Plaintiffs as a result of the cybersecurity incidents; identity theft protection for life; and the shutdown of every OPM information system until those systems satisfy the requirements of the Privacy Act and FISMA. CAC ¶¶ 208-15.

With respect to KeyPoint, the CAC alleges state law claims of negligence (Count Five), negligent misrepresentation and concealment (Count Six), invasion of privacy (Count Seven), violations of the Fair Credit Reporting Act (Count Eight), violations of various state statutes prohibiting unfair and deceptive trade practices (Count Nine), violations of various state data breach laws (Count 10), and state law breach of contract claims (Count Eleven).

3. Plaintiffs' Alleged Injuries and Damages

The thirty-eight individual Plaintiffs allege that they have sustained several categories of injuries as a result of the OPM cybersecurity incidents. These alleged injuries are listed on a plaintiff-by-plaintiff basis in paragraphs 13-50 of the CAC. For ease of reference, OPM has created a chart outlining the injuries and damages alleged by each of the thirty-eight Plaintiffs. *See* OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries. Plaintiffs allege the following six categories of injuries and damages in the CAC:

First, fifteen Plaintiffs allege that some form of fraudulent financial activity has occurred in their accounts after the cybersecurity incidents. The alleged fraud includes unauthorized charges on existing financial accounts (credit cards, debit cards, bank accounts), the fraudulent opening of new accounts (new credit and loan accounts), and unrecognized credit inquiries. These Plaintiffs allege that the fraudulent activity has caused them to spend time communicating with their financial institutions or other entities to reverse the fraudulent transactions or to close the fraudulent accounts.[6]

Second, seven Plaintiffs allege that an unidentified individual filed a fraudulent tax return using their personal information. These Plaintiffs allege that the fraudulent tax return has caused them to spend time resolving the fraud, and several Plaintiffs allege that their refund was delayed as a result of the filing of a fraudulent return.[7]

Third, four Plaintiffs allege that an unidentified individual misused or attempted to misuse their or their child's Social Security number, which caused the Plaintiffs to spend time resolving the issue.[8]

Fourth, all thirty eight Plaintiffs appear to allege that they face a heightened risk of future identity theft or other harm as a result of the cybersecurity incidents.[9]

---

[6] CAC ¶¶ 13 (Arnold), 14 (Bachtell), 16 (Bos), 19 (Burnett-Rick), 22 (Jane Doe), 28 (Flynn), 29 (Fuli), 30 (Gonzales), 31 (Gonzalez-Colon), 38 (King-Myers), 39 (Lozar), 41 (Oliver), 45 (Sharper), 49 (Wheatley), 50 (Winsor).

[7] CAC ¶¶ 14 (Bachtell), 21 (Daly), 24 (Doe), 26 (Doe III), 28 (Flynn), 31 (Gonzales-Colon), 32 (Griffith).

[8] CAC ¶¶ 14 (Bachtell), 17 (Branch), 41(Oliver), 50 (Winsor).

[9] For example, see CAC ¶ 7 (alleging that Plaintiffs' information is "subject to a continuing risk of additional exposure or theft as a consequence of OPM's ongoing failure to secure it"); *id.* ¶ 210 (alleging that "millions of government workers" are "at a heightened risk of identity theft, fraud, and other detrimental consequences); *id.* ¶ 134 (alleging that OPM's conduct "heightened the risk of a successful intrusion into OPM's systems"). In addition, every Plaintiff seeks credit monitoring

Fifth, thirty-four Plaintiffs allege that they have spent time and money on measures to protect against the risk of future identity theft or other harm. These alleged measures include reviewing financial accounts with greater frequency; purchasing credit monitoring services in addition to the services that the federal government has already provided; purchasing additional credit reports; placing credit freezes on accounts; and refraining from using online bill pay.[10]

Sixth, seventeen Plaintiffs allege that they suffer from some form of stress as a result of the cybersecurity incidents. Plaintiffs allege that they suffer from stress related to the possibility of future identity theft; stress related to career advancement, including the possibility that they will not be able to obtain a security clearance for government employment; and stress related to personal and family safety.[11]

III. Standards of Review

A. Rule 12(b)(1)

Motions brought pursuant to Rule 12(b)(1) challenge whether the district court has jurisdiction over the action. *See* Fed. R. Civ. P. 12(b)(1). "Federal courts are courts of limited jurisdiction," *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994), and thus a party claiming subject matter jurisdiction bears the burden of demonstrating that such jurisdiction exists,

---

services for their entire lifetime, *see id.* at 75, Prayer for Relief ¶ E, a request that is apparently premised on the future risk of some form of identity theft.

[10] CAC ¶¶ 13 (Arnold), 14 (Bachtell), 15 (Bonner), 16 (Bos), 17 (Branch), 18 (Brown), 19 (Burnett-Rick), 20 (Crawfod), 21 (Daly), 22 (Jane Doe), 25 (John Doe II), 26 (John Doe III), 27 (Ebert), 28 (Flynn), 29 (Fuli), 30 (Gonzales), 31 (Gonzales-Colon), 32 (Griffith), 33 (Gum), 34 (Hannagan), 36 (Hoffman), 37 (Johnson), 38 (King-Myers), 39 (Lozar), 40 (McGarry), 41 (Oliver), 42 (Peters), 43 (Sampredro), 44 (Sebert), 46 (Slater), 47 (Strickland), 48 (Uliano), 49 (Wheatley), 50 (Winsor).

[11] CAC ¶¶ 13 (Arnold), 18 (Brown), 19 (Burnett-Rick), 22 (Jane Doe), 23 (Jane Doe II), 24 (John Doe), 25 (John Doe II), 28 (Flynn), 30 (Gonzales), 31 (Gonzales-Colon), 35 (Hibbs), 37 (Johnson), 42 (Peters), 43 (Sampedro), 44 (Sebert), 46 (Slater), 50 (Winsor).

Khadr v. United States, 529 F.3d 1112, 1115 (D.C. Cir. 2008). Though a court must give the plaintiff the benefit of inferences that can be derived from the facts alleged in the complaint, *Barr v. Clinton*, 370 F.3d 1196, 1199 (D.C. Cir. 2004), "the Court need not accept factual inferences drawn by plaintiffs if those inferences are not supported by facts alleged in the complaint, nor must the Court accept plaintiffs' legal conclusions." *Speelman v. United States*, 461 F. Supp. 2d 71, 73 (D.D.C. 2006) (citation omitted). When a defendant raises an issue of subject matter jurisdiction under Rule 12(b)(1), the Court must resolve the jurisdictional issue before it proceeds to the merits of the plaintiff's claims. *See, e.g., Sinochem Int'l Co. v. Malay. Int'l Shipping Corp.*, 549 U.S. 422, 430-31 (2007).

B. Rule 12(b)(6)

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In reviewing a motion to dismiss under Rule 12(b)(6), the Court will ordinarily "accept as true all of the factual allegations contained in the complaint," *Atherton*, 567 F.3d at 681 (citation omitted), and construe it in plaintiff's favor. *Porter v. CIA*, 778 F. Supp. 2d 60, 65 (D.C. Cir. 2011). However, "the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions" or "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678.

C. Rule 9(g)

Federal Rule of Civil Procedure 9(g) requires that "an item of special damage" must be "specifically stated." "This heightened pleading standard applies because 'special damages,' unlike general damages, are 'not the necessary consequence of the defendant's conduct, but stem from the particular circumstances of the case.'" *Browning v. Clinton*, 292 F.3d 235, 245 (D.C. Cir. 2002) (internal alterations and citation omitted).

SUMMARY OF ARGUMENT

All claims in this multidistrict litigation should be dismissed for lack of subject matter jurisdiction because Plaintiffs have failed to establish Article III standing. Plaintiffs lack standing because they have failed to allege a cognizable injury-in-fact that is fairly traceable to OPM's conduct. The individual Plaintiffs allege that the OPM cybersecurity incidents caused six wide-ranging categories of injury: fraudulent financial activity in their accounts; fraudulent tax returns filed in a Plaintiff's name; misuse of Social Security numbers; the increased risk of future harm; time and money spent to protect against the risk of future harm; and emotional distress. None of these alleged injuries, however, is sufficient to establish an actual or imminent injury that is fairly traceable to OPM's conduct. This case therefore should be dismissed for lack of Article III standing.

Even if Plaintiffs had standing to pursue their claims, Plaintiffs' claims under the Privacy Act, Little Tucker Act, and the APA should be dismissed for multiple independent reasons.

Plaintiffs' Privacy Act claims for money damages should be dismissed because Plaintiffs have failed to plead facts showing that they have suffered pecuniary damages, *i.e.*, out-of-pocket financial loss. The Supreme Court has explicitly held that monetary loss is an essential element that must be specially pleaded, and the failure to plead actual damages is fatal to any claim seeking money damages under the Act. Plaintiffs' Privacy Act claims also should be dismissed because Plaintiffs do not plead sufficient facts showing that OPM engaged in intentional and willful conduct—the extremely high standard that must be met to establish culpability under the Privacy Act.

Plaintiffs' claims for breach of contract under the Little Tucker Act—which do little more than recast their Privacy Act claims in contract form—also should be dismissed. Plaintiffs base these claims on the Standard Form questionnaires they submitted to the government in connection with the processing of their background investigations. These questionnaires, however, do not constitute binding contracts for a variety of reasons. Most significantly, OPM's only alleged promise

in the questionnaires is a disclosure statement that informs any person submitting the form that his or her information will be treated in accordance with the requirements of the Privacy Act. It is well established that this type of alleged "promise to follow the law," which is no more than an informational statement describing the government's pre-existing legal obligations, is not enforceable in contract. In addition, even if these questionnaires did constitute binding contracts, such a contract would not reflect an intent to permit money damages in the event of a breach—which is a necessary requirement for jurisdiction under the Little Tucker Act.

Plaintiffs' claims for injunctive and declaratory relief under the APA also should be dismissed. Plaintiffs' APA claims fail because the APA cannot be invoked if another statute expressly or impliedly forbids the relief which is sought. Here, the Privacy Act provides specific remedies, which do not include injunctive relief for the claims alleged here, and Plaintiffs cannot avoid these limitations by invoking the APA. In addition, Plaintiffs also seek to enforce OPM's compliance with the Federal Information Security Management Act through the APA. However, the execution of this statute is committed to agency discretion by law and is not subject to APA review. Finally, to the extent Plaintiffs seek an injunction to compel agency action unlawfully withheld or unreasonably delayed, Plaintiffs fail to identify a final and discrete agency action required by law that OPM failed to take.

ARGUMENT

I. THIS CASE SHOULD BE DISMISSED FOR LACK OF SUBJECT MATTER JURISDICTION BECAUSE PLAINTIFFS LACK CONSTITUTIONAL STANDING.

Plaintiffs "carry the burden of establishing their standing under Article III," *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006), an obligation that "enforces the Constitution's case-or-controversy requirement." *Id.* (citation omitted). Indeed, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-

court jurisdiction to actual cases or controversies." *DaimlerChrysler*, 547 U.S. at 341 (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997)) (alteration in original). "If a dispute is not a proper case or controversy, the courts have no business deciding it, or expounding [on] the law in the course of doing so." *Id.* Accordingly, "when a federal court concludes that it lacks subject-matter jurisdiction, the court must dismiss the complaint in its entirety." *Arbaugh v. Y&H Corp.*, 546 U.S. 500, 514 (2006).

To establish standing, "a plaintiff must show (1) [she] has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical;
(2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envt'l. Serv. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000) (citing and quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)). In a putative class action such as this one, each of the named plaintiffs "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975); *see also O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) (class representative must have standing before he can seek relief on behalf of himself and another member of putative class). Further, Article III standing is claim- and relief-specific, such that a plaintiff must establish Article III standing for each claim and form of relief sought. *See DaimlerChrysler,* 547 U.S. at 352.

Standing is "always a case- and context-specific inquiry." *Nat'l Ass'n of Home Builders v. E.P.A.*, 786 F.3d 34, 43 (D.C. Cir. 2015) (citation omitted). Here, Plaintiffs allege that they have been injured because third-party wrongdoers have allegedly misused—or might in the future misuse—their personal information at some time following the intrusion into the information systems of OPM and its contractor. Plaintiffs do not allege who these third-party wrongdoers may

be, *i.e.* whether the alleged information misuse was or will be perpetrated by the cyber intruders themselves or by additional third parties who may obtain Plaintiffs' information from other sources. Under such circumstances, where third-parties commit the injurious acts upon which standing is claimed, causation hinges on the decisions of "independent actors not before the court" whose actions "the courts cannot presume either to control or predict." *Ctr. for Biological Diversity v. U.S. Dep't of Interior*, 563 F.3d 466, 477 (D.C. Cir. 2009) (citation omitted). In such cases, like this one, "where the [plaintiff] is not the object of an alleged government action or inaction, standing is not precluded, but it is ordinarily substantially more difficult to establish." *Id.* (citing *Lujan,* 504 U.S. at 562) Plaintiffs must plead "facts showing that those [third-party] choices have been or will be made in such manner as to produce causation and permit redressability of injury." *Id.* at 478 (citing *Lujan*, 504 U.S. at 562).

A. Plaintiffs Lack Standing To Pursue Money Damages For Alleged Past Harms.

The thirty-eight individual Plaintiffs cannot establish standing in this case because they cannot plead a cognizable injury-in-fact that is causally connected to OPM's conduct. The six categories of past injuries alleged by Plaintiffs are not cognizable injuries that are fairly traceable to OPM's conduct. Plaintiffs thus cannot establish standing, and this entire case should be dismissed for lack of subject matter jurisdiction.[12]

---

[12] As an initial matter, two pleading deficiencies affect the standing allegations of all Plaintiffs in this case, regardless of the specific category of alleged injury. First, at no point in the seventy-seven page Consolidated Amended Complaint does any Plaintiff identify what data incident they were subject to, *i.e.* the incident involving personnel records, the incident involving background-investigation records, or perhaps both incidents. The thirty-eight individual Plaintiffs each allege that they "received notice from OPM that [their] information had been compromised in the Data Breaches." *See* CAC ¶¶ 13-50. But Plaintiffs never identify what notice they received, despite the notifications being separate. This deficiency is significant because the two cybersecurity incidents involved different types of information. If a Plaintiff does not identify what incident he or she was allegedly

1. Fraudulent Financial Activity

Fifteen Plaintiffs allege that fraudulent financial activity has occurred in their individual accounts after the cybersecurity incidents.[13] Three types of fraud are alleged: unauthorized charges on existing bank accounts, credit cards, and debit cards; unauthorized charges on new credit and loan accounts that have been opened fraudulently in a Plaintiffs' name; and unrecognized credit inquiries. These Plaintiffs further allege that the fraud has caused them to spend time communicating with their financial institutions in order to reverse fraudulent transactions or to close fraudulently opened accounts. Plaintiffs do not allege, however, that they have been or ever will be required to pay for any fraudulent charges.

Plaintiffs' allegations fail to establish standing for two reasons. First, Plaintiffs never allege that any of this fraudulent activity caused them actual monetary loss. In analyzing whether fraudulent financial activity constitutes injury for purposes of Article III standing in data breach cases, courts have consistently held that only *unreimbursed* fraud that causes personal monetary loss can constitute injury-in-fact. *See, e.g.*, *Whalen v. Michael Stores Inc.*, No. 14-cv-7006, 2015 WL 9462108, at *3 (E.D.N.Y. Dec. 28, 2015) (holding that plaintiff failed to establish standing because she failed to allege that she was required to pay for alleged unauthorized charge); *Hammond v. The Bank of New*

---

subject to, then that Plaintiff cannot plausibly link any particular type of compromised information to a particular harm.

Second, the CAC includes a "catch-all" paragraph of alleged harms (commonly alleged in every data breach case) that unidentified plaintiffs and members of the putative class allegedly have sustained as a result of the cybersecurity incidents. *See* CAC ¶ 163. But this paragraph and its sub-paragraphs cannot establish standing. As noted, in a putative class action like this one, a plaintiff must allege that they have sustained a *personal* injury unique to them, not that injuries have been suffered by unidentified members of the putative class. *See Warth*, 422 U.S. at 502; *O'Shea*, 414 U.S. at 494 (1974).

[13] See *supra* note 6 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

.

York Mellon Corp., No. 08-cv-6060, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (holding that an unauthorized credit card charge for which a plaintiff is not held financially responsible is not an "injury" under Article III); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013) ("In order to have suffered an actual injury, [plaintiff] must have had an unreimbursed charge on her credit card. . . ."); *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1280–81 (N.D. Ala. 2014) (finding no standing despite plaintiff's allegations of unauthorized charges on his debit card because plaintiff did not allege that he actually had to pay for the charges).

Here, Plaintiffs allege that fraudulent transactions were made on their existing financial accounts or on new accounts that have been fraudulently opened, or that credit inquiries have been made by companies they do not recognize. But no Plaintiff ever alleges that this unauthorized financial activity has resulted in personal monetary loss. Not one Plaintiff alleges that his or her financial institution has found him or her to be liable for the fraudulent transactions, or that an unrecognized credit inquiry has impaired a particular Plaintiff's credit in any way. This is not surprising given that Congress long ago protected consumers from credit and debit card fraud, by providing a $50 limit to their liability. *See* 15 U.S.C. § 1643; 12 C.F.R. § 226.12. And, as a practical matter, almost every major card issuer in the country has a zero-fraud-liability policy and reimburses consumers for the $50 not covered by federal law. *See Whalen,* 2015 WL 9462108, at *3 (taking judicial notice of the fact that every major card issuer in the country has a zero-liability policy). In short, because Plaintiffs fail to allege that they have been or will be required to pay for the fraudulent charges imposed on their accounts, or that the fraudulent financial activity has caused them to suffer actual harm, Plaintiffs' allegations of unauthorized financial charges or unrecognized credit inquiries cannot establish standing. *See, e.g.*, *Whalen*, 2015 WL 9462108, at *3; *Hammond*, 2010 WL 2643307, at *8; *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *6; *Burton*, 47 F. Supp. 3d at 1280–81.

Second, Plaintiffs' allegations of fraudulent financial activity—whether on existing accounts, new accounts, or through unrecognized credit inquiries—do not establish standing because Plaintiffs do not plead facts plausibly showing that the fraud is fairly traceable to OPM's conduct, or even the particular incident.

As an initial matter, identity theft, especially in the form of fraudulent financial activity, is common in the United States. For instance, according to a 2015 report issued by the Department of Justice's Bureau of Justice Statistics, an estimated 17.6 million people, or 7 percent of all U.S. residents age 16 or older, were victims of some form of identity theft in 2014. Erika Harrell, *Victims of Identity Theft, 2014* (September 2015), U.S. Department of Justice, Bureau of Justice Statistics, http://www.bjs.gov/content/pub/pdf/vit14.pdf. Here, the intrusions into OPM's systems affected the data of approximately 22 million people and occurred at least a year ago, prior to April of 2015. Despite the enormous number of people affected and the significant amount of time that has elapsed, only a small subset of 15 individual Plaintiffs even allege that their financial information has been misused. In a society where 7 percent of the adult population will experience some form of identity theft each year, it is not surprising that at least 15 people out of a group of approximately 22 million happen to have experienced credit or bank-account fraud in the past year. Thus, the incidents of unauthorized charges—which millions of Americans experience every year through a wide variety of circumstances—is not indicative of data misuse that is fairly traceable to the OPM cybersecurity incidents. *See In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, No. 14-MD-2586, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016) ("Given the unfortunate frequency of credit card fraud, it is common sense to expect that in any group similar in size to the sixteen Plaintiffs and multitudes of potential class members . . . would likely experience at least one instance of a fraudulent charge."); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.* ("*SAIC*"), 45 F. Supp. 3d 14, 34 (D.D.C. 2014) ("To quantify that percentage, of the 4.7 million customers whose

data was [subject to the breach], one would expect around 155,100 of them to experience identity fraud simply by virtue of living in America and engaging in commerce, even if [the breach had never occurred].”). Indeed, Plaintiffs have not disclaimed any involvement in other data breaches, such as those frequently and recently experienced by commercial business or in the healthcare industry, which could have also affected those whose information was impacted by the OPM incidents.

Further, the instances of financial fraud alleged in the CAC are highly particular to each Plaintiff and do not suggest that they are causally connected to any data breach, let alone the OPM breaches. The alleged financial harms in the CAC range from incidents of fraud on an existing credit-card and bank accounts, to incidents of fraud on new online payday loan accounts, to wireless cellphone accounts, to electricity accounts, to unrecognized credit inquiries by unidentified companies. Plaintiffs make no effort whatsoever to allege how all of this disparate fraud is traceable to the information affected by the OPM cybersecurity incidents. They do not allege facts indicating that the intruders responsible for the OPM incidents committed these transactions, or that the intruders sold or exchanged compromised information to other criminals who perpetrated the fraud.

Nor is it apparent how the information that was affected in the OPM incidents could have led to fraud on an existing financial account. Plaintiffs never allege that the credit card number, debit card number, or other particular financial account number that was allegedly misused was compromised during the incidents. *See* CAC ¶¶ 67, 143-47. In addition, unlike most data breaches affecting commercial businesses or the healthcare industry, OPM is aware of “no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of federal personnel were impacted” by the incidents. OPM Announcement (July 9, 2015), Ex. 2 at 2. Further, Plaintiffs have not alleged that their submission of Standard From 86 would have included specific, active account information that would plausibly lead to the fraud alleged

here.[14] Nor do Plaintiffs allege facts that plausibly indicate that a criminal has used the information compromised in the OPM cybersecurity incidents to obtain a particular credit card number, debit card number, or financial account number that was misused. Thus, because no facts connect any incident of financial fraud to the OPM incidents, Plaintiffs' allegations of fraudulent financial activity do not establish standing. *See SAIC,* 45 F. Supp. 3d at 32 (finding the plaintiffs did not have standing based on allegations concerning the misuse of their bank accounts where they "proferr[ed] no plausible explanation for how the thief would have acquired their banking information."). Plaintiffs' allegations of fraudulent financial activity rest entirely on speculation about the actions of third-party wrongdoers and are insufficient to establish standing. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 (2013) (expressing "our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors"); *Ctr. for Biological Diversity,* 563 F.3d at 477 (citation omitted) (noting Plaintiffs' burden to plead facts plausibly showing that third-party "choices have been or will be made in such manner as to produce causation and permit redressability of injury.").

[14] Section 26 of Standard Form 86 does ask a variety of questions about an applicant's financial history pertinent to federal service, but it does not ask for specific, active account information that could plausibly be used to make the unauthorized charges Plaintiffs allege here. For example, Section 26 asks whether the applicant has ever filed a bankruptcy petition; experienced financial problems due to gambling; failed to file federal or state taxes; misused a travel or credit card provided by an employer; utilized a credit counseling service; or in the past seven years been delinquent on a variety of debts, including credit card debt. *See* Standard Form 86 (Revised December 2010), *Questionnaire for National Security Positions*, Section 26, U.S. Office of Personnel Management, https://www.opm.gov/forms/pdf_fill/sf86.pdf) (last visited May 13, 2016). Plaintiffs do not plausibly allege any explanation for how this type of information is the source of the alleged fraud.

2. Fraudulent Tax Returns

Seven Plaintiffs allege that an unidentified third party filed a fraudulent tax return in their name after the OPM incidents.[15] These allegations do not establish standing because no facts indicate that the tax fraud is fairly traceable to OPM.

As with identity-theft in general, the filing of fraudulent tax returns is a relatively common occurrence in the United States. For example, the IRS detected 3.7 million fraudulent tax returns in 2012 and 4.1 million in 2013—before the OPM incidents at issue here. *See* Treasury Inspector General for Tax Administration, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft*, at 3 (Apr. 24, 2015), https://www.treasury.gov/tigta/auditreports/2015reports/201540026fr.pdf. Given that millions of Americans are affected by the filing of fraudulent tax returns every year, it is not surprising that at least seven people out of a putative class of approximately 22 million would happen to have fraudulent tax returns filed in their name. *See SAIC*, 45 F. Supp. 3d at 32. And Plaintiffs' have alleged no facts suggesting that a fraudulent return is plausibly connected to the information compromised in the OPM incidents. Plaintiffs do not allege that the intruders responsible for the cybersecurity incidents at OPM are also filers of fraudulent tax returns, or that the intruders shared or sold particular categories of information to individuals who would likely file fraudulent returns. Plaintiffs, accordingly, cannot establish standing simply by alleging a false tax return has been filed in their name. *See*, *e.g.*, *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. 13-cv-7418, 2015 WL 1472483, at *8 (D.N.J. Mar. 31, 2015) (concluding that fraudulent tax return was not fairly traceable to particular data breach), *appeal docketed*, No. 15-2309 (3d Cir. June 1, 2015).

[15] *See* supra note 7 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

3. Misuse of Social Security Numbers

Four Plaintiffs allege that an unidentified individual misused or attempted to misuse their Social Security number ("SSN") after the OPM cybersecurity incidents.[16] Plaintiff Bachtell alleges that his SSN was used to open an unauthorized "My Social Security" account online (CAC ¶ 14); Plaintiff Branch alleges that the Social Security Administration notified him that an unknown individual had attempted to use his Social Security number, and that the incident required Branch to spend time verifying his identity and creating an identity theft profile with the Social Security Administration (CAC ¶ 17); and Plaintiff Winsor alleges that her credit monitoring service informed her that her minor son's SSN had been used in California for an unknown purpose (CAC ¶ 50).

These allegations fail to establish standing because Plaintiffs fail to allege facts plausibly showing that this activity is traceable to the data incidents at OPM. While it is true that SSNs were compromised in the OPM incidents, CAC ¶ 144, that fact hardly indicates that the OPM incidents led to these incidents of SSN misuse. Social Security numbers are used extensively in both the public and private sector. For instance, individuals must typically provide SSNs when applying for credit, when seeking medical or other insurance coverage, for leasing an apartment, seeking cell phone service, or applying for a job. *See* U.S. Gen. Accounting Office, GAO Rep. 99-28, *Social Security: Government and Commercial Use of the Social Security Number is Widespread*, (February 1999), *http://www.gao.gov/archive/1999/he99028.pdf* (last visited May 16, 2016). An identity thief can obtain a SSN by stealing a wallet or purse; opening an individual's mail; stealing the number from an unsecured website online; rummaging through trash at work or at home; posing by phone or email as someone who legitimately needs the information about you, such as employers or landlords; and buying personal information from "inside" sources, like a store employee processing credit

[16] *See* supra note 8 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

applications. *See Identity Theft and Your Social Security Number, Social Security Administration*, *https://www.ssa.gov/pubs/EN-05-10064.pdf*. Given the widespread use and misuse of SSNs, Plaintiffs must plead facts indicating why their alleged misuse is fairly traceable to the OPM incidents. Their failure to do so is fatal to their standing here.

4. Increased Risk of Future Harm

All Plaintiffs in this case appear to allege that they have been injured because they face a heightened risk of future harm as a result of the data incidents.[17] These allegations do not establish standing because they are only speculative claims of possible future injury, which are not sufficient to establish standing under Article III.

To satisfy the injury in fact element of standing, an injury must be "concrete, particularized, and actual or imminent." *Clapper,* 133 S. Ct. at 1147. When a party's alleged injury is based on future harm, standing exists if the threatened injury is "'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (*quoting Clapper*, 133 S. Ct. at 1147, 1150 n.5). "[A]llegations of *possible* future injury are not sufficient." *Clapper*, 133 S. Ct. at 1147 (citation omitted).

The requirement that a future injury be imminent "ensure[s] that the alleged injury is not too speculative for Article III purposes." *Lujan*, 504 U.S. at 564 n.2. Although imminence is a "somewhat elastic concept," it requires "that the injury proceed with a high degree of immediacy, so as to reduce the possibility of deciding a case in which no injury would have occurred at all." *Id.* (citation omitted). Additionally, where a threatened injury hinges on speculation about the actions of third parties, standing is less likely to exist. *See Clapper*, 133 S. Ct. at 1150 & n.5.

---

[17] *See* supra note 9 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

Applying these principles, this district court dismissed for lack of standing claims premised on increased risk of future harm in a data-breach case filed against a federal agency and its contractor. *SAIC*, 45 F. Supp. 3d 14 (D.D.C. 2014). Under *Clapper* and the law of this Circuit,[18] the court found that the only "question is whether the harm is certainly impending." *Id.* at 25 (citing and quoting *Pub. Citizen v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1297-98 (D.C. Cir. 2007) (""increased risk' is not by 'itself [a] concrete, particularized, and actual injury for standing purposes'—harm must be 'actual' or 'imminent,' not merely 'increased'")). And where, as here, plaintiffs allege that their information might be misused in the future, such allegations do not establish standing because the injury is not "certainly impending." Instead, the possible future injury is "entirely dependent on the actions of an unknown third party—namely, the thief," and/or additional third parties. *Id.* at 25.

This court's decision in *SAIC* is consistent with the holdings of the majority of courts addressing whether plaintiffs can establish standing in data breach cases. "In data security breach cases where plaintiffs' data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing." *In re SuperValu, Inc.*, 2016 WL 81792, at *4 (collecting cases); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954-55 (D. Nev. 2015); *Green v. eBay Inc.*, No. 14-CV-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 366-67 (M.D. Pa. 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 853-54 (S.D. Tex. 2015); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014); *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *3; *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 875

[18] "When analyzing questions of federal law, the transferee court should apply the law of the circuit in which it is located." *In re Temporomandibular Joint (TMJ) Implants Prods. Liab. Litig.*, 97 F.3d 1050, 1055 (8th Cir. 1996); *see also Murphy v. F.D.I.C.*, 208 F.3d 959, 965-66 (11th Cir. 2000) (same).

(N.D. Ill. 2014); *In re Horizon Healthcare Servs. Data Breach Litig.*, 2015 WL 1472483, at *5-7; *Tierney v. Advocate Health & Hosps. Corp.*, No. 13-cv-6237, 2014 WL 5783333, at *2 (N.D. Ill. Sept. 4, 2014), aff'd 797 F.3d 449 (7th Cir. 2015); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009); *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205-R, 2012 WL 2873892, at *5 (W.D. Ky. July 12, 2012).

This Court should follow the reasoning in *SAIC* and the numerous cases cited above and conclude that Plaintiffs cannot establish standing by alleging they face "a heightened risk of identity theft, fraud, and other detrimental consequences" as a result of the OPM cybersecurity incidents. CAC ¶ 210. These allegations of speculative future injury are not "actual or imminent" but rather "conjectural" and "hypothetical," and therefore insufficient to confer standing. *See Whitmore v. Arkansas*, 495 U.S. 149, 155, 158 (1990). Plaintiffs' allegations of future identity theft or other harm, like their allegations of past harms, are entirely speculative and contingent on the actions of third-party cybersecurity intruders and possibly other third-party criminals, including whether these third-party actors: (1) read, copied, and understood a particular individual Plaintiff's information (out of a group of over approximately 22 million people); (2) intend to commit future criminal acts by misusing the information; and (3) are able to use such information to the detriment of a particular Plaintiff. *In re SuperValu, Inc.*, 2016 WL 81792, at *5 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011); *SAIC*, 45 F. Supp. 3d at 25 (rejecting "increased risk" theory of standing because it is based entirely on the decisions of an independent actor—a data thief—whose actions the Court cannot predict or control). In addition to the speculation of *whether* future harm will ever materialize from the OPM cybersecurity incidents, it cannot be known *when* such harm will occur. *Id.*; *see also In re Zappos.com*, 108 F. Supp. 3d at 957 ("It is not enough that a credible threat may occur at some point in the future; rather, the threat must be impending.") (citing *Lujan*, 504 U.S. at 564); *see also*

Whitmore, 495 U.S. at 158. Plaintiffs, accordingly, cannot establish standing by alleging that they face a non-imminent risk that their information might be misused at an indefinite point in the future.

The few post-*Clapper* data-breach cases in which courts have found plaintiffs to have standing are non-binding, in the clear minority, and factually distinguishable because they concern allegations of substantial and widespread misuse of stolen financial account information. For example, in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015), hackers stole the credit card numbers of department store customers, and shortly after the breach, the company learned that 9,200 of the 350,000 cards affected by the breach "were known to have been used fraudulently." *Id.* at 690. Given that fraudulent charges were actually incurred on card numbers stolen in the breach, and that the hackers targeted the specific credit card accounts that later were misused, the Seventh Circuit found that plaintiffs could establish standing even after *Clapper*. *Id.* *See also Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016) (applying *Neiman Marcus* and concluding that plaintiffs had standing in data breach case involving theft of credit- and debit cards, where unauthorized charges occurred on those stolen cards shortly after the breach); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (similar); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (similar).

In contrast to *Nieman Marcus*, this case does not involve the targeted theft of payment card information, nor does this case involve like factual allegations of widespread debit or credit card fraud tied very closely in time to a particular breach of a financial database storing active account information. *Nieman Marcus* thus provides no support for the conclusion that Plaintiffs in this

matter face any injury that is "certainly impending" for purposes of Article III standing. *See Clapper*, 133 S. Ct. at 1146.[19]

5. Time and Money Spent to Protect Against Future Identity Theft or Other Harm

Thirty-four Plaintiffs allege that they have sustained injury because they have taken measures to protect against the future risk of identity theft.[20] These alleged measures include reviewing financial accounts with greater frequency; purchasing credit monitoring services in addition to the monitoring and insurance services that the federal government has already provided; purchasing additional credit reports; placing credit freezes on accounts; and refraining from using online bill pay.

Plaintiffs' allegations do not establish standing under *Clapper*. As the Supreme Court explained, plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 133 S. Ct. at 1151 (citation omitted). "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.* In data breach cases, "courts consistently hold that the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent." *In re SuperValu, Inc.*, 2016 WL 81792, at *7; *see also SAIC*, 45 F. Supp. 3d at 26; *In re Zappos.com*, 108 F. Supp. 3d at 960-61. Here, the risk of future harm being mitigated is not

---

[19] *Nieman Marcus* also provides no support for Plaintiffs' ability to state a cognizable claim for relief against OPM. Although the Seventh Circuit concluded that Plaintiffs alleged sufficient facts to establish Article III standing, the panel never addressed whether the complaint in that case stated a claim on which relief may be granted. 794 F.3d at 697. As we discuss in Sections II-IV below, even if a particular Plaintiff could establish Article III standing, their claims should be dismissed because they fail state a cognizable claim for relief against OPM.

[20] *See* supra note 10 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

imminent. Thus, the cost to mitigate the risk is not a sufficient injury in fact to confer Article III standing.[21]

In addition, Plaintiffs' contention that they must spend their own money to protect against future harm—whether in the form of credit monitoring, credit reports, or credit freezes—is without basis because the federal government has already provided at no cost to Plaintiffs a comprehensive suite of protective services and identity-theft insurance to individuals affected by the OPM cybersecurity incidents, and Congress has extended these benefits for at least 10 years. *See* Consolidated Appropriation Act of 2016, § 632, 129 Stat. at 2470-71. Plaintiffs may decide to purchase additional services or take other precautions, if they so choose. But such decisions to voluntarily incur costs for a particular type of service cannot itself be the basis for standing to sue OPM. *Clapper*, 133 S. Ct. at 1151; s*ee also*, *e.g.*, *Fair Emp't Council of Greater Wash., Inc. v. BMC Mktg. Corp.*, 28 F.3d 1268, 1277 (D.C. Cir. 1994) (explaining that self-inflicted injuries are inadequate for standing).

6. Emotional Distress

Seventeen Plaintiffs allege that they suffer from some form of stress as a result of the data incidents.[22] Specifically, Plaintiffs allege that they suffer from stress related to the possibility of future identity theft; stress related to career advancement, including the possibility that they will not

---

[21] Even before *Clapper*, numerous courts, including this court, found that an "allegation that [plaintiffs] have incurred or will incur costs in an attempt to protect themselves against their alleged increased risk of identity theft fails to demonstrate an injury that is sufficiently 'concrete and particularized' and 'actual or imminent.'" *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007) (quoting *Lujan*, 504 U.S. at 560); *see also Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *5 n.7 (E.D. Pa. Mar. 9, 2010); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011); *Giordano v. Wachovia Secs., LLC*, No. 06-476, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006); *Key v. DSW Inc.*, 454 F. Supp. 2d 684, 688 (S.D. Ohio 2006); *Bell v. Acxiom Corp.*, No. 06-485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006).

[22] *See* supra note 11 & OPM Ex. 3, Chart of Plaintiffs' Alleged Damages and Injuries.

be able to obtain a security clearance for government employment; and stress related to personal and family safety, including the safety of their minor children.

Plaintiffs' alleged emotional distress is insufficient to establish standing. Courts have consistently held that "[e]motional distress in the wake of a security breach is insufficient to establish standing, particularly in a case that does not involve an imminent threat to the information." *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *5; *see also Reilly*, 664 F.3d at 44-46; *Low v. LinkedIn Corp.*, 11-CV-1468, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011). Here, Plaintiffs have not alleged facts showing the requisite imminence. Plaintiffs alleging concerns about future identity theft plead no facts plausibly suggesting that identity theft will imminently occur as a result of the OPM cybersecurity incidents, as discussed above. To be sure, well over a year after the incidents occurred, only a handful of individuals allege that they have experienced some form of identity theft, and these Plaintiffs plead no facts that plausibly show these experiences are connected to the OPM cybersecurity incidents. Plaintiffs alleging concerns about career advancement do not plead facts plausibly indicating that their career will be hindered or that their request for a security clearance will be denied as a result of the OPM incidents (which affected millions of federal employees), and they certainly have not alleged facts showing that such risks are imminent. And Plaintiffs who allege concerns about personal and family security fail to allege facts plausibly indicating that these individuals face an imminent threat of bodily harm as a result of the OPM incidents.[23] Because Plaintiffs have not pled facts showing that the information stolen during the

[23] An anonymous Plaintiff – Jane Doe (CAC ¶ 22) – alleges that the FBI "informed Doe that her GII had been acquired by the so-called Islamic State of Iraq and al-Sham ("ISIS")." CAC ¶ 22. This is of course a serious allegation. But Plaintiff Jane Doe alleges absolutely no facts indicating that ISIS obtained her information as a result of the OPM incidents, nor does she indicate that the FBI told her that ISIS obtained her information as the result of the incidents.

OPM cybersecurity incidents plausibly will be used to commit a crime in the imminent future, or will be used to hinder one's career in the imminent future, Plaintiffs' alleged stress following the incidents cannot establish standing.

B. Plaintiffs Lack Standing to Pursue Declaratory and Injunctive Relief for Alleged Future Harms.

In addition to seeking money damages for past harms under the Privacy Act and the Little Tucker Act, Plaintiffs seek prospective declaratory and injunctive relief under the APA. CAC ¶¶ 196-207. The injunctive relief sought by Plaintiffs is sweeping. They seek to enforce, through the APA, unspecified provisions of FISMA—a broad federal statute that provides "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). More specifically, Plaintiffs provide a laundry list of twelve actions that they argue OPM should have taken before and after the incidents in order to comply with FISMA's requirement that it establish an adequate data security program. *See* CAC ¶¶ 82–83, 200, 202. To remedy these alleged deficiencies, they ask the

---

Similarly, Jane Doe II (CAC ¶ 23) alleges that her husband is a federal prosecutor responsible for prosecuting cases against "international drug cartels known to target prosecutors, law enforcement officials, and their families" and she further alleges that her husband received "multiple death threats throughout his career and was the subject of an assassination attempt." But she alleges no facts at all indicating that international drug cartels or those who may wish harm have obtained her husband's information as a result of the OPM incidents.

Plaintiff Burnett-Rick (CAC ¶ 19) alleges that her work email address "had been found on the 'dark web'"—which consists of parts of the World Wide Web that cannot be accessed through standard technology and that is "predominantly used to facilitate illicit activities, such as drug trafficking and identity theft." But she alleges no facts indicating that the OPM incidents caused her email address to make its way to the dark web, or how having an email address on the dark web would cause her to suffer imminent harm.

With respect to concerns about the safety of minor children, the complimentary identity protection and credit monitoring services offered by OPM extends to minor children of those impacted by the background investigation records incident. *See* OPM's website (https://www.opm.gov/cybersecurity/) under the tab "Supporting people who have been affected."

Court to order "OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA," including by shutting down "all unauthorized information systems" until those systems are "validly authorized." *Id.* ¶ 215.

Plaintiffs' claims under the APA have numerous legal deficiencies. Most fundamentally, these claims should be dismissed because they cannot satisfy the well-established standing requirements necessary to seek prospective injunctive relief.[24]

To establish standing for future injunctive or declaratory relief, a plaintiff must do more than demonstrate past exposure to illegal conduct; he or she must demonstrate that there is a real and immediate threat that injury will be repeated in the absence of the requested injunctive relief being granted. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *Fair Emp't Council of Greater Wash., Inc.*, 28 F.3d at 1273 (holding that *Lyons* applies to requests for declaratory relief); *see also Worth v. Jackson*, 451 F.3d 854, 858 (D.C. Cir. 2006); *Reilly*, 664 F.3d at 42-43 (3d Cir. 2011); *Chang v. United States*, 738 F. Supp. 2d 83, 88 (D.D.C. 2010). Plaintiffs have not met that burden. Specifically, Plaintiffs have not alleged facts sufficient to establish a real and immediate threat that, unless their requested injunctive relief is granted, the same kind of cyberattack on OPM's systems will occur, and that this future attack will result in Plaintiffs' personal information being obtained and used in a harmful manner.

The Supreme Court articulated the standing requirements for injunctive relief in the seminal case *City of Los Angeles v. Lyons*, 461 U.S. 95 (1983). In *Lyons*, a plaintiff sought to enjoin the Los Angeles Police Department from using chokeholds except in limited circumstances. *Lyons*, 461 U.S. at 97–98. In support of his assertion that he had standing for injunctive relief, Mr. Lyons alleged that (1) he had been choked in the past; (2) city police regularly and routinely apply chokeholds with

[24] The other bases for dismissing Plaintiffs' APA claims are discussed in Section III below.

no provocation; (3) there had been at least 15 chokehold-related deaths; and (4) he therefore "justifiably fear[ed] that any contact he ha[d] with Los Angeles police officers may result in his being choked[.]" *Id.* at 98. The Supreme Court held that this was not sufficient to establish standing for Mr. Lyons to seek injunctive relief. In particular, the Court explained that the likelihood that the plaintiff would be subject to future chokeholds was conjectural because it rested on contingent events occurring at some time in the future; namely, that plaintiff himself would again be stopped by the police and would again be choked without any provocation or legal excuse. *Id.* at 106. The Court noted that even if it was likely that the police would illegally use chokeholds in the future, it could not be assumed that Mr. Lyons himself would be subjected to that treatment.

Here, Plaintiffs allege that they have standing to seek injunctive relief because: (1) OPM has previously incurred data security breaches, CAC ¶¶ 125–30; (2) federal agencies, including OPM, have been the subject of many attempted data security breaches, *id.* ¶¶ 79–80, 134; (3) Plaintiffs' personal information, along with that of millions of other individuals, is maintained in OPM's systems, *id.* ¶ 52; and (4) Plaintiffs' personal information therefore "remains at imminent risk of being exposed and stolen," *id.* ¶ 206.

These allegations do not establish standing for injunctive relief under *Lyons*. Indeed, the causal chain providing the basis for Plaintiffs' standing is even more conjectural than that in *Lyons*. First, to the extent Plaintiffs suggest that they currently suffer from the effects of OPM's alleged past non-compliance with FISMA, this allegation fails to establish standing for injunctive relief. "To pursue an injunction or a declaratory judgment, the . . . plaintiffs must allege a likelihood of future *violations* of their rights by [defendant], not simply future *effects* from past violations." *Fair Emp't Council of Greater Wash., Inc.*, 28 F.3d at 1273; *Nat. Res. Def. Council v. Pena*, 147 F.3d 1012, 1022 (D.C. Cir. 1998) ("Because respondent alleges only past infractions of [the statute], and not a continuing violation or the likelihood of a future violation, injunctive relief will not redress its injury.")

(quotation omitted). Second, the possibility that a particular Plaintiff might suffer from future injury, in the form of identity theft or other fraud, relies on a "highly attenuated chain of possibilities . . . . that rest on speculation about the decisions of independent actors." *Clapper* 133 S. Ct. at 1148, 1150. Here, the particular deficiencies identified by Plaintiffs have to be grave enough that they present a "real and immediate" threat that another extraordinary cyberattack will happen in the imminent future, and Plaintiffs have done no more than to broadly assert that attempts at unauthorized electronic intrusions are common. *See SAIC*, 45 F. Supp. 3d at 25 (no standing where future harms depend on actions of independent third-party thief). Third, none of the named Plaintiffs have alleged facts showing that such a breach, if it were to occur, is likely to result in injury to them personally. *See Ctr. for Biological Diversity*, 563 F.3d at 478 ("[I]t is well-established that a party must demonstrate that it has suffered an injury that affects it in a 'personal and individual way." (citation omitted)).

In sum, Plaintiffs have failed to allege that, unless the Court grants their requested injunction, another unidentified intruder will imminently and successfully perpetrate an additional intrusion, that Plaintiffs' data will be stolen as a result of that intrusion, and the unidentified intruder or separate wrongdoer will subsequently use that data in a manner that will cause Plaintiffs concrete harm. Plaintiffs' conclusory allegations, which largely rely on the general allegation that data security breaches are common, are not sufficient to establish standing for injunctive and declaratory relief.

C. Plaintiff AFGE Lacks Representational Standing Because It Fails to Identify At Least One Individual Member Who Has Standing.

As Sections I.A and I.B explain, no individual Plaintiff can establish standing to assert claims for money damages under the Privacy Act and the Little Tucker Act, or claims for future injunctive and declaratory relief under the APA. The failure of an individual plaintiff to establish standing is also fatal to AFGE's representational standing in this case. To establish representational standing,

an organization bringing a claim on behalf of its members must allege, among other things, that "its members would otherwise have standing to sue in their own right." *Nat'l Ass'n of Home Builders v. E.P.A.*, 667 F.3d 6, 12 (D.C. Cir. 2011) (internal quotation marks omitted). Because AFGE has failed to allege facts that a particular member has suffered an injury-in-fact that would provide standing to sue in his or her own right, AFGE cannot establish standing here.

II. PLAINTIFFS FAIL TO MEET THE REQUIREMENTS OF THE PRIVACY ACT.

Even if Plaintiffs could establish standing under Article III, their Privacy Act claims, which seek money damages, must be dismissed. CAC ¶¶ 175-85.[25]

The Privacy Act does not create a cause of action against the government equivalent to a general negligence claim for tortious conduct under the common law. It also does not authorize recovery where a plaintiff can only show that he or she has suffered general (as opposed to specific) damages. Instead, as the Supreme Court has explained in *FAA v. Cooper*, 132 S. Ct. 1441, 1453 (2012), particular standards govern any claim for money damages brought under the Privacy Act.

First, the Privacy Act requires a plaintiff to plead and prove that he or she has suffered out-of-pocket monetary loss. The Privacy Act provides that, for any "intentional or willful" refusal or failure to comply with the Act, the United States shall be liable for "*actual damages sustained by the individual* as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000." 5 U.S.C. § 552a(g)(4)(A)(emphasis added). As a result, to recover

---

[25] The Privacy Act does not authorize injunctive or declaratory relief for the claims Plaintiffs assert under 5 U.S.C. § 552a(g)(1)(D) and (g)(4). *See Kelley v. FBI*, 67 F. Supp. 3d 240, 253 (D.D.C. 2014) (citing *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007) ("We have held that only monetary damages, not declaratory or injunctive relief, are available to § 552a(g)(1)(D) plaintiffs . . ."). Recognizing that injunctive and declaratory relief is unavailable under the Privacy Act, Plaintiffs seek to obtain injunctive relief under the APA. CAC ¶¶ 196-207 (Count 3). But as we explain in Section IV below, a plaintiff cannot avoid the limited remedial scheme in the Privacy Act by repackaging the claim under the APA.

money damages under the Act, including the $1,000 statutory award, the plaintiff must first plead and prove that he or she has individually sustained "actual damages." *Cooper*, 132 S. Ct. at 1450-51; *Doe,* 540 U.S. at 620, 627. The term "actual damages" is "limited to proven pecuniary or economic harm." *Cooper*, 132 S. Ct. at 1453. The United States retains sovereign immunity for all non-economic harms, including "loss of reputation, shame, mortification, injury to the feelings and the like." *Id.* at 1441, 1451, 1453, 1456. The failure to establish monetary damage is fatal to Privacy Act claims under 5 U.S.C. § 552a(g)(1)(D) and (g)(4). *Cooper*, 132 S. Ct. at 1450-51; *Earle v. Holder*, No. 11-5280, 2012 WL 1450574, at *1 (D.C. Cir. Apr. 20, 2012).

Second, actual damages under the Privacy Act must be pled with specificity as required by Federal Rule of Civil Procedure 9(g). Rule 9(g) requires that, "[i]f an item of special damage is claimed, it must be *specifically stated*." Fed. R. Civ. P. 9(g) (emphasis added). In *Cooper*, the Supreme Court explained that the remedial scheme in the Privacy Act parallels the remedial scheme of certain defamation torts at common law—namely, libel per quod and slander—that require the pleading and proof of special damages. 132 S. Ct. at 1451; *id* at 1452 ("[W]e think it likely that Congress intended 'actual damages' in the Privacy Act to mean special damages for proven pecuniary loss."). Accordingly, as with defamation claims, the actual damages used to support a Privacy Act claim must be "*specially pleaded* and proved." *Id.* at 1451 (emphasis added).

Third, the concept of sovereign immunity requires the Court to construe any ambiguity regarding the scope of available damages in the Privacy Act in favor of the United States. *Id.* at 1448; *see also Tomasello v. Rubin*, 167 F.3d 612, 618 (D.C. Cir. 1999). As the Supreme Court emphasized in *Cooper* when discussing the limitations imposed by the Privacy Act:

> We have said on many occasions that a waiver of sovereign immunity must be "unequivocally expressed" in statutory text. . . . Any ambiguities in the statutory language are to be construed in favor of immunity, so that the government's consent to be sued is never enlarged beyond what a fair reading of the text requires.

> Ambiguity exists if there is a plausible interpretation of the statute that would not authorize money damages against the Government.

Cooper, 132 S. Ct. at 1448 (citations omitted). As such, to the extent there is any ambiguity in whether a particular category of damages alleged by Plaintiffs is compensable under the Privacy Act, that doubt must be resolved in the government's favor.

A. Plaintiffs Fail To Specifically Plead Actual Damages.

1. Plaintiffs' Allegations of Financial Fraud, Fraudulent Tax Returns, and Social Security Number Misuse Fail To Establish Actual Damages.

Plaintiffs assert three categories of injury that could arguably give rise to the type of out-of-pocket monetary loss that can form the basis for a Privacy Act claim—fraudulent financial activity, fraudulent tax returns, and misuse of Social Security numbers. But Plaintiffs have not alleged facts sufficient to demonstrate that they have in fact suffered such loss because of the OPM cybersecurity incidents.[26]

Most fundamentally, Plaintiffs' allegations fail to establish actual damages because Plaintiffs never allege that the fraudulent activity they describe has resulted in personal monetary loss. The Privacy Act only waives sovereign immunity for "actual damages *sustained by the individual* as a result of" an intentional and willful violation of the Act. 5 U.S.C. § 552a(g)(4)(A)(emphasis added). Here, some Plaintiffs allege that unauthorized charges have occurred on their existing financial accounts or on new accounts that have been fraudulently opened, that fraudulent tax returns have been filed in their name, and that their Social Security numbers have been misused. But these Plaintiffs never claim that the alleged misconduct caused them personal monetary loss. Plaintiffs, for example, have

---

[26] *Cooper* strongly supports the conclusion that actual damages must be pled with particularity and specificity under Rule 9(g). But even if the Court were to conclude that Rule 9(g) does not apply to pleading actual damages under the Privacy Act, Plaintiffs' allegations of actual damages do not satisfy the general pleading standards of Rule 8. Plaintiffs fail to plead facts plausibly showing that they have sustained actual monetary loss as a result of a Privacy Act violation.

not alleged that their financial institutions refused to reimburse the unauthorized transactions on their accounts or that they have been denied a refund due to the filing of a fraudulent tax return. This type of information, regarding Plaintiffs' own alleged losses, is in Plaintiffs' possession and there is no reason that they should have failed to meet these specific pleading requirements—unless, as is likely, no such losses have in fact been incurred.

Plaintiffs, moreover, have failed to plead facts showing that the fraudulent activity about which they complain was proximately caused by a violation of the Privacy Act. In order to bring a claim for monetary relief under the Privacy Act, the plaintiff must show that a federal agency's intentional and willful violation of the Act proximately caused her actual damage. *See* 5 U.S.C. § 552a(g)(4) (stating that actual damages must be "sustained by the individual *as a result of*" an intentional and willful violation of the Act); *Skinner v. U.S. Dep't of Justice*, 584 F.3d 1093, 1097 (D.C. Cir. 2009) (requiring Privacy Act plaintiff to show proximate causation). Here, Plaintiffs have not pled any facts connecting the alleged misuse of their financial information to the OPM cybersecurity incidents.

As discussed above in the context of Article III standing, Plaintiffs allegations with respect to causation are deficient for numerous reasons. *See supra* Section I.A.1–3. In summary:

(1) a substantial amount of the population will experience some form of identity theft every year, and thus simply experiencing identity theft, especially in the form of fraudulent financial activity, is not itself sufficient to allege that the fraud was caused by a particular data breach;

(2) the instances of financial fraud, fraudulent tax returns, and Social Security number misuse alleged in the CAC are highly particular to each Plaintiff, vary from one Plaintiff to the next, and thus do not suggest that the fraud is causally connected to one data breach, let alone the OPM incidents;

(3) Plaintiffs' allegations of existing-account fraud are especially deficient because no facts indicate that the credit card number, debit card number, or other financial account number that was allegedly misused was stolen during the data breaches, and Plaintiffs do not specifically state facts indicating how a criminal could have

> obtained a particular financial account number by using information that was stolen.

These allegations, which are not sufficient to establish Article III causation, also do not establish proximate cause under the Privacy Act. As noted, the Privacy Act provides a limited waiver of sovereign immunity and, as such, any ambiguity regarding the scope of available damages must be construed in favor of the United States. *Cooper*, 132 S. Ct. at 1448; *see also Tomasello*, 167 F.3d at 618. More specifically, in order for Plaintiffs to state a causal connection for their money-damages claim, they must show that the Privacy Act "unequivocally authorize[s]" the damages they seek, not simply that such damages are conceivably recoverable under the Act. *Cooper*, 132 S. Ct. at 1456. Here, even if one could conceive of a remote causal connection between the OPM cybersecurity incidents and the alleged harms, the Privacy Act certainly does not unequivocally authorize an award of damages for such speculative harms.[27]

2. Plaintiffs' Self-Inflicted Expenses Do Not Constitute Actual Damages

Plaintiffs additionally allege that they have sustained actual damages because they must take measures to protect against the future risk of identity theft. These measures include spending an increased amount of time reviewing credit reports; purchasing credit monitoring services, in addition to the monitoring and insurance services that the federal government has already provided; purchasing additional credit reports; incurring fees to place credit freezes on certain financial

[27] Plaintiffs also allege that they have suffered emotional harm and a heightened risk of future harm as a result of the incidents. OPM assumes that these allegations are intended only to support Plaintiffs' (incorrect) assertion that they have Article III standing to bring suit against the government and not to show that they have suffered actual damages under the Privacy Act. However, to the extent that they do assert this as a basis for demonstrating actual damages, such allegations are clearly insufficient because such alleged injuries do not constitute pecuniary or economic harm. *Cooper*, 132 S. Ct. 1441, 1446, 1451–53; *see also id.* 1456 (holding that because the Privacy Act "does not unequivocally authorize an award of damages for mental or emotional distress," it "does not waive the Federal Government's sovereign immunity from liability for such harms").

accounts; and refraining from using online bill pay and incurring fees to make payments over the telephone. None of these alleged harms constitutes actual damages under the Privacy Act.

First, none of these are harms proximately caused by a past Privacy Act violation; instead, they are all prophylactic measures taken to protect against the future risk of financial fraud or other harm. As explained in the context of Article III standing, a Plaintiff cannot manufacture present injury by incurring costs to prepare for a speculative future event. *Clapper*, 133 S. Ct. at 1151. That same principle applies with even greater force in evaluating actual damages under the Privacy Act. A Plaintiff cannot manufacture actual damages caused by a past Privacy Act violation simply by spending money to prepare for possible future harms. If that were the standard, then a plaintiff could always, and quite easily, manufacture actual damages—with its associated $1,000 statutory damage provision—by spending a few dollars on credit monitoring services, credit reports, or credit freezes. Such a standard would be inconsistent with the principle that waivers of sovereign immunity are to be interpreted narrowly, *see Cooper*, 132 S. Ct. at 1448, and in strong tension with *Clapper*'s holding that money spent in the anticipation of future harm is not injury-in-fact, *see* 133 S. Ct. at 1151. Accordingly, none of the measures Plaintiffs have taken to prevent possible future harm establish actual damages under the Privacy Act.

Further, Plaintiffs' contention that they must spend money to protect against future harm—whether in the form of credit monitoring, credit reports, or credit freezes—is without basis because the federal government has already provided a comprehensive suite of protective services to everyone affected by the OPM incidents, and Congress has extended these benefits for at least a decade. Plaintiffs are free to purchase additional services, if they so choose, but they can hardly argue that this voluntarily-incurred cost is the result of a Privacy Act violation. Nor does the Privacy Act "unequivocally authorize" an award of damages for future economic harms or harms already protected against through the Government's own expenditures.

B. Plaintiffs Fail To Plead Sufficient Facts Showing OPM Intentionally and Willfully Violated The Privacy Act.

In addition to their failure to allege actual damages, Plaintiffs also fail to allege facts making plausible their assertion that OPM's alleged violation of the Privacy Act was intentional and willful, a standard that Plaintiffs must meet to maintain this cause of action. Plaintiffs allege that OPM violated two provisions of the Privacy Act—the disclosure provision, 5 U.S.C. § 552a(b), which prevents with certain exceptions a federal agency from disclosing "any record . . . contained in a system of records" without the written consent of the "individual to whom the record pertains," and the safeguards provision, 5 U.S.C. § 552a(e)(10), which requires federal agencies to "establish appropriate administrative, technical, and physical safeguards" in order to protect agency records. CAC ¶¶ 182-83. Both allegations are deficient.

1. Applicable Law

To assert a Privacy Act claim for money damages against the United States under 5 U.S.C. § 552a(g)(1)(D) and (g)(4), a plaintiff must plead and prove that "the agency acted in a manner which was intentional or willful." 5 U.S.C. § 552a(g)(4); *see also Kelley v. FBI*, 67 F. Supp. 3d 240, 253-54 (D.D.C. 2014). The words "intentional" and "willful" in § 552a(g)(4) "do not have their vernacular meanings; instead, they are terms of art." *Kelley,* 67 F. Supp. 3d at 257 (citation omitted). To meet the "intentional" and "willful" standard under section 552a(g)(4), as applied in this Circuit, an agency must either commit an act "without grounds for believing it to be lawful" or act in a manner that "flagrantly disregard[s] others' rights under the Act." *Albright v. United States*, 732 F.2d 181, 189 (D.C. Cir. 1984).

Under this extremely high standard of culpability, a plaintiff must allege agency action that is "so '*patently egregious and unlawful*' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham v. U.S. Navy*, 813 F.2d 1236, 1242 (D.C. Cir. 1987) (quoting *Wisdom v. Dep't of*

Hous. & Urban Dev., 713 F.2d 422, 425 (8th Cir.1983)) (emphasis added). The Court of Appeals has explained that this standard of culpability requires a showing that the agency acted in a manner "*greater* than gross negligence." *Waters v. Thornburgh*, 888 F.2d 870, 875 (D.C. Cir. 1989) (quoting Analysis of House and Senate Compromise Amendments to the Federal Privacy Act, 120 Cong. Rec. 40,405, 40,406 (1974)) (emphasis added). If, as here, a plaintiff cannot plead facts showing the agency acted with the requisite culpability, then a Privacy Act claim seeking money damages under § 552a(g)(4) must be dismissed. *See*, *e.g.*, *Kelley*, 67 F. Supp. 3d at 267; *Dick v. Holder*, 67 F. Supp. 3d 167, 186 (D.D.C. 2014); *Doe v. U.S. Dep't of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009).

2. Plaintiffs Fail To Allege that Defendant Intentionally and Willfully Violated the Disclosure Provision of the Privacy Act

Plaintiffs' complaint is completely devoid of allegations suggesting that OPM intentionally and willfully disclosed their information in violation of the Privacy Act, 5 U.S.C. § 552a(b). The disclosure provision of the Act provides that no agency shall "disclose" an individual's records "to any person, or to another agency," without the individual's consent, unless a particular statutory exception authorizes the disclosure. *See* 5 U.S.C. § 552a(b). The Circuit has explained that the term "disclose" in the Privacy Act involves an agency's decision to intentionally and willfully transmit a protected record to another person or another agency without authorization. *See Pilon v. U.S. Dep't of Justice*, 73 F.3d 1111, 1124 (D.C. Cir. 1996) ("Our review of the Privacy Act's purposes, legislative history, and integrated structure convinces us that Congress intended the term 'disclose' to apply in virtually all instances to an agency's unauthorized transmission of a protected record, regardless of the recipient's prior familiarity with it."). No such disclosure is alleged to have occurred here.

Plaintiffs instead allege that their records were stolen by third-party cyber intruders in a "sophisticated" and "malicious" attack on OPM's information systems. *See* CAC ¶¶ 114-37. This third party may well have acted intentionally and willfully in perpetrating this breach. But Plaintiffs

do not allege (nor could they allege) that OPM collaborated with this third party for the purpose of disclosing Plaintiffs' records. In the absence of such allegations, Plaintiffs' disclosure claim cannot survive. As another court in this district has explained in rejecting a disclosure claim based on the malicious conduct of a third party:

> It is difficult to imagine how an illegal act of a third party over whom the [agency] had no control could nevertheless constitute an intentional or willful disclosure by the [agency]. Plaintiffs cite no cases supporting their theory that a theft can be a willful and intentional disclosure, nor have they pled any facts that, if true, would support that conclusion.

In re Dep't of Veterans Affairs (VA) Data Theft Litig., No. 06-0506, 2007 WL 7621261, at *6 (D.D.C. Nov. 16, 2007). The same is true here. Plaintiffs have not alleged any facts that would suggest that OPM had any control over the acts of third-party wrongdoers or otherwise colluded with these wrongdoers.

Plaintiffs, in fact, make clear that their disclosure claim is simply a recycled and repackaged version of their safeguards claim. *See id.* (explaining that allegations supporting a safeguards claim under 5 U.S.C. § 552a(e)(10) cannot be "recycled and re-pled" under the disclosure provision of the Privacy Act, 5 U.S.C. § 552a(b)). Plaintiffs not only collapse both their safeguards claim and disclosure claim into a single count, they also claim that the alleged "disclosure" was the "direct and proximate result" of OPM's alleged "non-compliance with federal requirements and its intentional disregard of the IG's findings under FISMA." CAC ¶ 183. Putting aside whether such allegations can support their safeguards claim, there is no logical basis for the suggestion that OPMs decision not to adopt certain safeguards constitutes an intentional decision to disclose Plaintiffs' records.

3. Plaintiffs Fail To Allege Sufficient Facts Showing that OPM Intentionally and Willfully Violated the Safeguards Provision of the Privacy Act

Plaintiffs' claim under the safeguards provision of the Privacy Act, 5 U.S.C. § 552a(e)(10), is also legally deficient and should be dismissed. Section (e)(10) of the Privacy Act directs agencies to "establish appropriate administrative, technical, and physical safeguards" in order to keep records secure and to guard against anticipated security threats that could substantially harm, embarrass, inconvenience, or cause unfairness to an individual for whom an agency record is maintained. 5 U.S.C. § 552a(e)(10). As noted, to state a claim for money damages based on the alleged violation of this provision, Plaintiffs must plead facts showing OPM acted "intentionally" and "willfully." *See* 5 U.S.C. § 552a(g)(4). Plaintiffs, accordingly, must plead facts showing OPM committed an act "without grounds for believing it to be lawful" or acted in a manner that "flagrantly disregard[s] others' rights under the Act." *Albright*, 732 F.2d at 189. In other words, Plaintiffs must allege facts showing that OPM acted in a manner that is "so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham*, 813 F.2d at 1242 (citation omitted). The Privacy Act "does not make the Government strictly liable for every affirmative or negligent action [of an employee] that might be said technically to violate the Privacy Act's provisions." *Albright*, 732 F.2d at 189; *see also White v. Shafer*, 738 F. Supp. 2d 1121, 1142 (D. Colo. 2010), aff'd, 435 F. App'x 764 (10th Cir. 2011).

Here, the essence of Plaintiffs' safeguards claim is that OPM did not adequately or immediately implement some of the discretionary cybersecurity improvements recommended by OPM's Office of Inspector General as part of its FISMA audit. CAC ¶ 178-80. But the Privacy Act does not impose monetary liability on the United States simply because a federal agency decides not to implement certain discretionary cybersecurity improvements—a decision that must be based on a host of administrative, operational, and budgetary concerns. In addition, as Plaintiffs' own allegations show, an agency's information security program is extremely complex, interconnected, and constantly evolving. For example, Plaintiffs complain in this case about OPM's decisions with

respect to two-factor identification, firewalls, software authorizations, and cybersecurity structures. CAC ¶ 180. But regardless of whether OPM made the correct decision with respect to these very complex and technical matters, these decisions simply do not rise to the level of conduct "so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful." *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007) (quoting *Deters v. U.S. Parole Comm'n*, 85 F.3d 655, 660 (D.C. Cir. 1996)).

Plaintiffs' allegations also fail to account for the fact that the Privacy Act affords agencies discretion in implementing its requirements. Although the Privacy Act requires OPM to "establish appropriate administrative, technical, and physical safeguards to" protect Plaintiffs' personal information, 5 U.S.C. § 552a(e)(10), the statute does not mandate the establishment of any specific safeguard, and agencies have broad discretion to decide what "safeguards" to implement to protect personal information. *See In re Dep't of Veterans Affairs Data Theft Litigation*, 2007 WL 7621261, at *4 ("[T]he Privacy Act does not prescribe specific technical standards, leaving agencies to manage their own information security[.]"); *Kostyu v. United States*, 742 F. Supp. 413, 417 (E.D. Mich. 1990) (the Privacy Act affords agencies "broad discretion to cho[o]se among alternative methods of securing their records commensurate with their needs, objectives, procedures, and resources."); *see also* S. Rep. No. 93-1183 (1974), as reprinted in 1974 U.S.C.C.A.N. 6916. Congress did not require agencies to adopt "a general set of technical standards for security of systems. Rather, the agency is merely required to establish those administrative and technical safeguards which it determines are appropriate and finds technologically feasible for the adequate protection of the confidentiality of the particular information it keeps against purloining, unauthorized access, and political pressures to yield the information improperly to persons with no formal need for it." *Id.* (quoting S. Rep. No. 93-1183). Given the considerable discretion that federal agencies have in implementing Privacy Act safeguards, OPM's alleged decision not to immediately implement every recommendation in the

OIG annual FISMA audit does not rise to the level of willful and intentional conduct required by the Act. Therefore, Plaintiffs safeguards claims should be dismissed.

III. PLAINTIFFS FAIL TO MEET THE REQUIREMENTS OF THE LITTLE TUCKER ACT.

Plaintiffs' breach-of-contract claims—which do little more than recast their Privacy Act claims in contract form—should likewise be dismissed. Plaintiffs bring these claims on behalf of themselves and others who submitted SF-85, SF-85 P, and SF-86 questionnaires to OPM in connection with their background investigations. *See* CAC ¶¶ 186-95.[28] These claims should be dismissed for a variety of reasons—including because the questionnaires do not create any substantive legal rights beyond the Privacy Act that would permit Plaintiffs to seek redress from the government.

A. The Submission of the Questionnaires Did Not Create Binding Contracts Between the Parties

Plaintiffs have failed to allege plausibly the existence of an express or implied contract between the parties. According to Plaintiffs, they agreed to provide their personal information to the government in exchange for OPM's agreement to protect their information from unauthorized disclosure. *See* CAC ¶¶ 189–90. The disclosure statements that Plaintiffs cite as the source of this alleged contractual promise, however, serve the much more limited purpose of notifying any person submitting a background investigation questionnaire that his or her information will be treated in

[28] The Standard Forms (SF 85, 85P, and 86) are available at OPM's website: https://www.opm.gov/forms/federal-investigation-forms/(last visited May 13, 2016). The Court may consider these forms in ruling on OPM's Rule 12(b)(6) motion to dismiss because the CAC incorporates them by reference. *SeeUnited States v. Sci. Applicatons Int'l Corp.*, 502 F. Supp. 2d 75, 78 (D.D.C. 2007) (quoting *Air Line Pilots Ass'n v. Delta Air Lines*, 863 F.2d 87, 94 (D.C. Cir. 1988)). Alternatively, the Court may also take judicial notice of these publicly available government documents. *See Detroit Int'l Bridge Co. v. Gov't of Canada*, 133 F. Supp. 3d 70, 84-85 (D.D.C. 2015) ("[J]udicial notice may be taken of public records and government documents available from reliable sources.") (citation omitted).

accordance with the requirements of the Privacy Act. Because a promise to follow a pre-existing legal obligation cannot form the basis for a contractual agreement, Plaintiffs' breach-of-contract claims should be dismissed.

Plaintiffs' assertion that there is a contract between the parties is based on three substantially similar "Disclosure of Information" statements in the questionnaire forms that inform applicants of the governing law. The SF-86, for example, states in relevant part:

> **Disclosure [of] Information**
>
> The information you provide is for the purpose of investigating you for a national security position, and the information will be protected from unauthorized disclosure. *The collection, maintenance, and disclosure of background investigative information are governed by the Privacy Act.* The agency that requested the investigation and the agency that conducted the investigation have published notices in the Federal Register describing the *systems of records* in which your records will be maintained. The information you provide on this form, and information collected during an investigation, *may be disclosed without your consent by an agency maintaining the information in a system of records as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine use, a list of which are published by the agency in the Federal Register.* The office that gave you this form will provide you a copy of its routine uses.

SF-86 at 2 (emphasis added).

As is apparent on its face, the purpose of this disclosure statement is to inform the applicant that his or her information will be treated in accordance with the Privacy Act. In addition to expressly stating that the collection, maintenance, and disclosure of background investigation information are governed by the Privacy Act, the statement notifies the applicant of that statute's relevant provisions. Among other things, the statement informs applicants that: (1) government agencies must give public notice of their systems of records by publication in the Federal Register; (2) the applicant's information is to be maintained in those systems of records; and (3) the applicant's information may be disclosed pursuant to certain exceptions. Each of these substantive legal obligations is provided for by the Privacy Act.

Such a statement cannot serve as the basis of a contractual agreement because a promise to abide by the law cannot serve as consideration. *See* Restatement (Second) of Contracts § 73 (1981) ("Performance of a legal duty owed to a promisor which is neither doubtful nor the subject of honest dispute is not consideration[.]"); *Allen v. United* States, 100 F.3d 133, 134 (Fed. Cir. 1996) ("Performance of a pre-existing legal duty is not consideration.") (citation omitted); *Youngblood v. Vistronix, Inc.*, No. 05-21, 2006 WL 2092636, *4 (D.D.C. July 27, 2006) ("It is a general maxim of contract law that a party cannot offer as consideration a duty that the party is already obligated to perform.") (citation omitted); *Floyd v. United States*, 26 Cl. Ct. 889, 891 (1992) ("That which one is under a legal duty to do, cannot be the basis for a contractual promise.") (citation omitted), *aff'd,* 996 F.2d 1237 (Fed. Cir. 1993). The government has a pre-existing and ongoing legal obligation to comply with the requirements of the Privacy Act. The questionnaires neither add to, nor detract from, that obligation and do not reflect a bargained-for agreement between the parties.[29]

The disclosure statement in the questionnaires, in fact, is best understood not as a contractual promise but as a notification. Government forms regularly inform their users of the governing legal framework that is applicable to a particular form. The inclusion of such a notification does not create a contractual obligation, *see Tripp v. United States*, 257 F. Supp. 2d 37, 47-48 (D.D.C. 2003) (holding that the mention of Privacy Act obligations at the end of a security

---

[29] Even if Plaintiffs could somehow establish that the questionnaires reflect some implicit contractual obligation for services beyond the statutory protections of the Privacy Act (which they cannot), their breach-of-contract claims fail because they have not alleged facts establishing the elements of a contract with the United States—including (1) mutuality of intent to contract; (2) consideration; and (3) lack of ambiguity in offer and acceptance, and when the United States is a party, a showing that the government representative whose conduct is relied upon had actual authority to bind the government. *See City of El Centro v. United States*, 922 F.2d 816, 820 (Fed. Cir. 1990). Indeed, Courts have routinely found that the government's invitation to fill out a standard form is not an offer to contract. *See Chattler v. United States*, 632 F.3d 1324 (Fed. Cir. 2011); *XP Vehicles, Inc. v. United States*, 121 Fed. Cl. 770, 785 (2015).

clearance application form does not create a contractual obligation), and interpreting such statements in that manner would likely have the undesirable consequence of discouraging their inclusion.

At bottom, although Plaintiffs have tried to recast their claims for damages under the law of contract, it is clear that the real legal source of their claims is the Privacy Act. But Plaintiffs cannot use the Little Tucker Act to circumvent the limitations to the Privacy Act. It is well established that the Privacy Act does not create a substantive right to money damages enforceable under the Little Tucker Act. *See*, *e.g.*, *Snowton v. United States*, 216 F. App'x 981, 983 (Fed. Cir. 2007); *accord Rebish v. United States*, 120 Fed. Cl. 184, 188 (2015).[30] As the Supreme Court has explained,

> The Tucker Act is displaced . . . when a law assertedly imposing monetary liability on the United States contains its own judicial remedies. In that event, the specific remedial scheme establishes the exclusive framework for the liability Congress created under the statute.

Bormes, 133 S. Ct. at 18. As discussed above, the Privacy Act provides a comprehensive remedial scheme—which, among other things, requires Plaintiffs to plead and prove that they have suffered actual damages in order to recover any loss. Plaintiffs should not be permitted to borrow the more general waiver of sovereign immunity from the Little Tucker Act, and avoid that requirement, by recasting their claim in the law of contract. *Id.* at 19 ("Plaintiffs cannot, therefore, mix and match FCRA's provisions with the Little Tucker Act's immunity waiver to create an action against the United States."). "[If plaintiffs] may not sue under the statute, it would make scant sense to allow

---

[30] *See also Madison v. United States*, 98 Fed. Cl. 393, 395 (2011); *Treece v. United States*, 96 Fed. Cl. 226, 232 (2010); *Stephanatos v. United States*, 81 Fed. Cl. 440, 444-45 (2008); *Henderson v. United States*, No. 07-677C, 2007 WL 5173635, at *2-4 (Fed. Cl. Oct. 16, 2007); *Parker v. United States*, 77 Fed. Cl. 279, 291-92 (2007), *aff'd*, 280 F. App'x 957 (Fed. Cir. 2008) (all finding no jurisdiction to bring a Privacy Act claim under the Tucker Act).

them to sue on a form contract implementing the statute, setting out terms identical to those contained in the statute." *Astra USA, Inc. v. Santa Clara Cty.*, 563 U.S. 110, 114 (2011).

B. There is No Applicable Waiver of Sovereign Immunity Because Plaintiffs Have Not Identified A Substantive Right to Money Damages

Even if the submission of these questionnaires could somehow be construed as creating a contract between the parties, which it cannot, Plaintiffs have not identified an applicable waiver of sovereign immunity to bring a claim seeking redress for the breach of that purported contract. The Little Tucker Act, on which Plaintiffs rely, only provides a waiver of immunity to bring a breach-of-contract claim where the underlying contract is money mandating. But, as discussed, there is nothing in the questionnaires indicating that OPM intended to enter into a contract with Plaintiffs at all, let alone that it intended to enter into a contract that would permit an award of money damages.

To bring a claim against the government, a plaintiff must identify an unequivocally expressed waiver of sovereign immunity. *See Bormes,* 133 S. Ct. at 16. The Little Tucker Act does not itself create a substantive right to recover damages. *Id.* at 15. It is a jurisdictional provision that operates to waive sovereign immunity for certain monetary claims based on other sources of law—including, in some circumstances, contracts between private parties and the government. *Id.* at 16.[31] But, as

---

[31] The Little Tucker Act, 28 U.S.C. § 1346, provides, in relevant part:

> (a) The district courts shall have original jurisdiction, concurrent with the United States Court of Federal Claims, of:
>
> * * *
>
> (2) Any other civil action or claim against the United States, not exceeding $10,000 in amount, founded either upon the Constitution, or any Act of Congress, or any regulation of an executive department, or upon any express or implied contract with the United States, or for liquidated or unliquidated damages in cases not sounding in tort . . . .

the Federal Circuit explained, the "government's consent to suit under the [Little] Tucker Act does not extend to every contract." *Rick's Mushroom Serv., Inc. v. United States*, 521 F.3d 1338, 1343 (2008) (citation omitted). It only applies where the underlying agreement provides a substantive right to recover money damages. *Id.*

Though there is generally a presumption that a damages remedy will be available when a contract has been breached, where there is doubt that the government has made a statement triggering monetary liability, a plaintiff seeking to bring suit must identify specific provisions of the agreement that contemplate an award of money damages. *See Higbie v. United States*, 778 F.3d 990 (Fed. Cir. 2015) (affirming denial of Tucker Act jurisdiction over claimed breach of a mediation agreement because contract was not money mandating). Courts, for example, have declined to hold that agreements are money mandating where the agreement makes no provision for money damages, *Rick's Mushroom*, 521 F.3d at 1343; concerns the conduct of parties in a criminal case, *Sanders v. United States,* 252 F.3d 1329, 1336 (Fed. Cir. 2001); contains an express disavowal of the availability of money damages, *Holmes v. United States,* 657 F.3d 1303, 1314 (Fed. Cir. 2011); or contemplates injunctive relief for a breach, *Higbie*, 778 F.3d at 993.

That same analysis applies here. A government agency's statement on a questionnaire form that an applicant's information will be treated in accordance with federal law is not the type of promise that, if broken, would be presumed to entitle a party to contract damages. *See Pressman v. United States*, 33 Fed. Cl. 438, 444 (1995) ("The violation of the statute or regulation will not be enforceable through a contract remedy.") (citation omitted), *aff'd*, 78 F.3d 604 (Fed. Cir. 1996); *Army & Air Force Exch. Serv. v. Sheehan*, 456 U.S. 728 (1982) (Tucker Act jurisdiction cannot be premised on asserted violation of employment regulations that do not specifically authorize money damages).

And Plaintiffs have not identified any provision of those questionnaires that would suggest money damages are appropriate. In the absence of Plaintiffs identifying such provisions (which they cannot), there is no basis for this Court to find that the government has entered into an agreement that provides a substantive right to damages that may be enforced under the Little Tucker Act.

IV. PLAINTIFFS FAIL TO MEET THE REQUIREMENTS OF THE ADMINISTRATIVE PROCEDURE ACT

In Count Three, Plaintiffs seek injunctive relief against OPM under the APA, 5 U.S.C. §§ 702-706. CAC ¶ 198. As discussed in Section I, Plaintiffs' APA claim should be dismissed for lack of standing. However, even if Plaintiffs could establish standing, their APA claim still should be dismissed because: (1) the Privacy Act precludes Plaintiffs' request for injunctive and declaratory relief under the APA; (2) Plaintiffs' APA claim, which seeks to enforce unspecified provisions of FISMA, does not state a claim because OPM's compliance with FISMA is committed to agency discretion by law and thus not subject to APA review; and (3) Plaintiffs fail to identify a discrete agency action required by law that OPM failed to take.

A. The Privacy Act Precludes Plaintiffs' Requested Injunctive Relief under The APA

The APA generally waives the federal government's immunity from a lawsuit "seeking relief other than money damages and stating a claim that an agency or an officer or employee thereof acted or failed to act in an official capacity or under color of legal authority." 5 U.S.C. § 702. That waiver of immunity, however, "comes with an important carve-out[.]" *Patchak*, 132 S. Ct. at 2204-05. It "cannot be invoked where another statute 'expressly or impliedly forbids the relief which is sought.'" *Kelley,* 67 F. Supp. 3d at 267 (citing 5 U.S.C. § 702). As the Supreme Court has explained, "[t]hat provision prevents plaintiffs from exploiting the APA's waiver to evade limitations on suit contained in other statutes." *Patchak*, 132 S. Ct. at 2204-05; *see also Block v. North Dakota ex rel. Bd. of Univ. & School Lands*, 461 U.S. 273, 286 & n.22 (1983); *cf.* 5 U.S.C. § 704 (permitting review of "final

agency action for which there is no *other* adequate remedy in a court") (emphasis added). "[W]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy—including its exceptions—to be exclusive, that is the end of the matter; the APA does not undo the judgment." *Patchak*, 132 S. Ct. at 2205 (citing *Block*, 461 U.S. at 286 & n.22).

Plaintiffs may not use the APA to obtain relief for Privacy Act violations that Congress has not made part of the Privacy Act's comprehensive remedial scheme. The Privacy Act authorizes injunctive relief in only two specific circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C §§ 552a(g)(1)(A), (g)(2)(A), and (2) to order an agency to allow an individual access to his records, *id.* § 552a(g)(1)(B). Several courts have established that the equitable remedies for Privacy Act violations are limited to those specifically identified in the statute. *See Cell Assocs., Inc. v. Nat'l Institutes of Health*, 579 F.2d 1155, 1161-62 (9th Cir. 1978)*; Edison v. Dep't of the Army*, 672 F.2d 840, 846-47 (11th Cir. 1982) (citing *Parks v. IRS*, 618 F.2d 677, 683-84 (10th Cir. 1980)); *Houston v. U.S. Dep't of Treasury*, 494 F. Supp. 24, 29 (D.D.C. 1979); *cf. Kelley*, 67 F. Supp. 3d at 252. These holdings are consistent with the principle that "[w]here [a] 'statute provides certain types of equitable relief but not others, it is not proper to imply a broad right to injunctive relief.'" *Parks*, 618 F.2d at 684 (citing *Cell Assocs.*, 579 F.2d at 1161-62). This is especially true with the Privacy Act because Congress "link[ed] particular violations of the Act to particular remedies in a specific and detailed manner[,]" which "points to a conclusion that Congress did not intend to authorize the issuance of [other] injunctions." *Cell Assocs.*, 579 F.2d at 1158.

Following these well-established principles, numerous federal courts, including this court, have concluded that the Privacy Act precludes injunctive relief under the APA, and thus a plaintiff cannot bring an APA claim to obtain injunctive relief for an alleged Privacy Act violation. *See, e.g., Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014); *Wilson v. McHugh*, 842 F. Supp. 2d 310, 320 (D.D.C. 2012); *Doe P v. Goss*, No. 04-2122, 2007 WL 106523, at *6 n.8 (D.D.C. Jan. 12, 2007); *Reid v.*

Fed. Bureau of Prisons, No. 04-1845, 2005 WL 1699425, at *2 (D.D.C. July 20, 2005); *Mittleman v. U.S. Treasury*, 773 F. Supp. 442, 449 (D.D.C. 1991); *Mittleman v. King*, No. 93-1869, 1997 WL 911801, at *4 (D.D.C. 1997)); *Arruda & Beaudoin, LLP v. Astrue*, No. 11-10254, 2013 WL 1309249, at *15 (D. Mass. March 27, 2013); *Ware v. U.S. Dep't of Interior*, No. 05-3033, 2006 WL 1005091, at *3 (D. Or. Apr. 14, 2006); *Schaeuble v. Reno*, 87 F. Supp. 2d 383, 393-94 (D.N.J. 2000) (citing *Mittleman v. United States Treasury*, 773 F. Supp. 442, 449 (D.D.C. 1991)); *Diaz-Bernal v. Myers*, 758 F. Supp. 2d 106, 119 (D. Conn. 2010); *El Badrawi v. Dep't of Homeland Sec.*, 579 F. Supp. 2d 249, 280 n.35 (D. Conn. 2008).[32]

In sum, Plaintiffs should not be allowed to circumvent the limited equitable remedies that Congress has authorized for Privacy Act violations by improperly invoking the APA. The APA is a limited waiver of sovereign immunity that is strictly construed in favor of the Government, and it does not confer authority to grant injunctive relief for Privacy Act violations beyond the relief specifically provided in the Privacy Act.

B. OPM's Compliance with FISMA Is Committed to Agency Discretion by Law and thus Not Subject to Judicial Review under the APA

Even if Plaintiffs could bring an APA claim predicated on alleged violations of the Privacy Act, the relief they seek is not available under the APA. In their Complaint, Plaintiffs seek to enforce through the APA unspecified provisions of the FISMA and regulations and technical standards for data security issued by OMB and NIST.[33] CAC ¶¶ 198-206. These allegations do not

---

[32] OPM is aware of one contrary district court decision permitting a plaintiff to bring an independent APA claim based on a Privacy Act violation. *See Radack v. U.S. Dep't of Justice*, 402 F. Supp. 2d 99, 104 (D.D.C. 2005). This outlier decision is incorrect, however, as it conflicts with §§ 702 and 704 of the APA, the principles enunciated by the Supreme Court, as well as the decisions of dozens of other federal courts.

[33] Plaintiffs do not seek to assert a claim directly under FISMA, nor could they. FISMA does not create a cause of action for private litigants. *See, e.g, Sci. Sys. & Applications, Inc. v. United States*, No.

state a claim because the APA provides no cause of action to review OPM's compliance with its responsibilities under FISMA. Instead, a federal agency's compliance with FISMA is committed to agency discretion by law.

The judicial review provisions of the APA, 5 U.S.C. §§ 701–06, establish a cause of action for parties adversely affected either by agency action or by an agency's failure to act. *Chaney*, 470 U.S. at 828. However, the APA explicitly excludes from judicial review those agency actions that are "committed to agency discretion by law." 5 U.S.C. § 701(a)(2). "Because the APA does not apply to agency action committed to agency discretion by law, a plaintiff who challenges such an action cannot state a claim under the APA." *Oryszak v. Sullivan*, 576 F.3d 522, 525 (D.C. Cir. 2009).

The Supreme Court has identified "at least two occasions" in which agency action is committed to agency discretion by law and thus not subject to APA review: "[I]n those rare instances where statutes are drawn in such broad terms that in a given case there is no law to apply," *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971), and "when the statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion," *Chaney*, 470 U.S. at 830. *See Sierra Club v. Jackson*, 648 F.3d 848, 855 (D.C. Cir. 2011). Agency actions in these circumstances are unreviewable because "the courts have no legal norms pursuant to which to evaluate the challenged action, and thus no concrete limitations to impose on the agency's exercise of discretion." *Sierra Club*, 648 F.3d at 855 (citing *Sec'y of Labor v. Twentymile Coal Co.*, 456 F.3d 151, 156 (D.C. Cir. 2006)).

To determine whether a matter has been committed to agency discretion, the D.C. Circuit considers "the language and structure of the statute that supplies the applicable legal standards for

---

14–CV-2212, 2014 WL 3672908, at *2 (D. Md. July 22, 2014); *United States ex rel. Vasudeva v. Dutta-Gupta*, No. CA CV-114 ML, 2014 WL 6811506, at *12 (D.R.I. Dec. 2, 2014).

reviewing that action" and "the nature of the administrative action at issue." *Sierra Club*, 648 F.3d at 855 (citing *Twentymile Coal*, 456 F.3d at 156); *see also Drake v. F.A.A.*, 291 F.3d 59, 70 (D.C. Cir. 2002). Here, both factors support the conclusion that an agency's decisions implementing FISMA are committed to agency discretion and not reviewable under the APA. Indeed, the D.C. Circuit has examined the statutory structure of FISMA and suggested in extensive dicta that the choices an agency makes in carrying out its FISMA obligations are not subject to judicial review. *See Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) ("Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations.").

1. The Language and Structure of FISMA Indicate that FISMA Compliance Is Committed to Agency Discretion by Law

The language and structure of FISMA indicate that an agency's choices in implementing its information-security responsibilities are not subject to judicial review under the APA. Congress passed FISMA to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). However, Congress specifically "recognize[d] that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products." 44 U.S.C.A. § 3551(6).

Accordingly, while FISMA imposes general obligations on agencies to develop and implement information security protections, it offers no specific prescriptions for the tools or methods required—which is unsurprising, in light of the rapidly evolving nature of both technology and cyber threats. Instead, Congress vested agencies with broad discretion to adopt "security protections commensurate with the risk and magnitude of the harm" resulting from cyber threats. 44 U.S.C. § 3554(a)(1)(A). FISMA gives agencies latitude to develop security policies and

procedures that are "appropriate" and "cost-effectively reduce information security risks to an acceptable level." *Id.* at 3554(b)(2)(B).

To achieve its goals, FISMA assigns *exclusive* responsibility for overseeing the management and security of information systems of civilian agencies to the Director of the Office of Management and Budget. FISMA mandates that the OMB Director "shall oversee agency information security policies and practices, including . . . overseeing agency compliance with the requirements of this subchapter [of FISMA.]" *Id.* § 3553(a)(5). FISMA specifically authorizes the OMB Director "to enforce accountability for compliance," *id.* § 3553(a)(5), through various mechanisms, including by "tak[ing] any action that the Director considers appropriate, including an action involving the budgetary process or appropriations management process." 40 U.S.C. § 11303(b)(5)(A). Additionally, the Director must review each agency's security programs at least annually and approve or disapprove them. 44 U.S.C. § 3553(a)(5). Finally, he must report to Congress annually on the "effectiveness of information security policies and practices during the preceding year." *Id.* § 3553(c).

The legislative history confirms that OMB is responsible for enforcing FISMA across civilian federal agencies, not the federal courts. In a Senate Committee on Homeland Security and Governmental Affairs report updating the Act, the Committee stated that:

> Under FISMA, the Director of OMB has *exclusive authority to oversee the management and security of information security across federal civilian agencies*. These functions include developing and overseeing information security policies, principles, standards and guidelines, requiring agencies to identify and provide information security protections commensurate with risk, and *overseeing agency compliance with the requirements of FISMA*, among other things.

S. Rep. No. 113-256, at *3 (2014) (emphasis added).

In complying with their obligations under FISMA, the Director of OMB and agency heads must also ensure compliance with information security standards promulgated by the Department of

Commerce. *See*, *e.g.*, 44 U.S.C. §§ 3553(a)(1)-(2), 3554(a)(1)(B)(i) (incorporating the requirements of 40 U.S.C. § 11331). The Director of OMB must, "on the basis of proposed standards developed by the National Institute of Standards and Technology" ("NIST"), and "in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems." 40 U.S.C. § 11331(b)(1)(A). The NIST, in turn, is required by statute to "consult with other agencies and offices" (including at least six enumerated agencies) when developing its standards and guidelines. 15 U.S.C. § 278g–3(c)(1). The purpose of such collaboration is to "improve information security and avoid unnecessary and costly duplication of effort," as well as to ensure that the standards and guidelines "are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems." *Id.* § 278g–3(c)(1)(A),(B). The NIST's standards and guidelines must not require "specific technological solutions or products" and must "permit the use of off-the-shelf commercially developed" products as much as possible. *Id.* § 278g–3(c)(5),(7). The NIST must give the public a chance to comment on proposed standards and guidelines, *id.* § 278g–3(c)(2), and must provide agencies with assistance with implementation, *id.* § 278g–3(d)(2).

FISMA, in short, is "nestled . . . within this multilayered statutory scheme." *Cobell,* 455 F.3d at 314. It includes a role for numerous entities, including OMB, the Department of Commerce, the Department of Homeland Security, the NIST, the Comptroller General, Congress, the public (by way of notice and comment), and multiple officials within each agency subject to the statute. But nowhere did Congress indicate that the federal courts should review the information-security decisions made by these numerous entities. *See id.* ("Notably absent from FISMA is a role for the judicial branch.") FISMA, accordingly, is precisely the type of statute whose "language and structure" indicate that Congress intended for its implementation to be committed to agency discretion by law and thus not subject to APA review.

2. The Discretionary and Technical Nature of an Agency's Information-Security Program Indicates That FISMA Is Committed to Agency Discretion by Law

The nature of the administrative action challenged here—OPM's implementation of its information-security program under FISMA—also supports a finding that such agency action is not subject to review under the APA. In their Complaint, Plaintiffs seek to challenge a host of decisions that OPM has made with respect to its information-security program, all of which are highly technical and discretionary in nature. *See* CAC 200. For instance, Plaintiffs seek judicial review of OPM's decision to operate certain computer and software systems without "valid authorizations"; whether to use "multi-factor authentication" for a particular system; the appropriate implementation of "adequate network and data segmentation"; the appropriate use of "layered security defenses, such as firewalls and host level anti-malware"; whether OPM "adequately and continu[ously] monitor[ed] security controls and their effectiveness"; whether OPM properly "elect[ed] not to encrypt sensitive personal information under its control"; whether OPM properly implemented a centralized "structure for governance and management of information security"; whether OPM "provid[ed] its employees with []adequate training in electronic security techniques, defenses and protocols"; and had "a comprehensive inventory of its servers, databases and network drives." CAC ¶ 200. Plaintiffs also seek to set aside three OPM alleged decisions not to "shut down or otherwise isolate the compromised electronic systems"; "undertake measures to identify, disrupt, or limit the ongoing attacks on its systems"; and "change the access codes used to gain entry into its systems[]" subsequent to the breaches. *Id.* ¶ 202. Finally, Plaintiffs also apparently seek to compel OPM to correct general deficiencies noted in the November 2015 OIG audit, including: "that an outbound web proxy is still missing at OPM, that controls have not been implemented to prevent unauthorized devices from connecting to the OPM network," and "that OPM's vulnerability management program remains substandard." *Id.* ¶ 205.

Plaintiffs fail to identify any rules or guidance that impose mandatory requirements on OPM to implement any specific controls or actions related to the named IT security improvements. Overarching OMB guidance on FISMA implementation makes clear that agencies are required to adopt "adequate security," but that "adequate security" is a flexible concept that includes considerations of effective operation and cost-effective management.[34] Consistent with that flexible framework, the Secretary of Commerce issues "compulsory and binding" IT security guidance via documents called Federal Information Processing Standards Publications ("FIPS"). *See* 40 U.S.C. § 11331 (b)(1); 44 U.S.C. § 3553(a)(1,2). But the FIPS do not require agencies to adopt specific security controls either, but rather direct that agencies "must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements," and that "[t]he process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve *adequate security* [as defined by OMB] is a multifaceted, risk-based activity involving management and operational personnel within the organization."[35] Additional non-binding guidance and recommendations as to IT security policies under FISMA are principally laid out in documents called Special Publications ("SPs") that are issued by the NIST. Although OMB policy requires agencies such as OPM to follow NIST SPs, the SPs themselves acknowledge that "[o]rganizations have flexibility in applying the baseline security

[34] OMB Circular A-130, App'x III, at A(2)(a) (defining "adequate security" as including "assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls"), https://www.whitehouse.gov/omb/circulars_a130_a130trans4/.

[35] See FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems (Mar. 2006), Section 4, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf., Id. at 4.

controls" and that organizations must "tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation."[36]

The wide-ranging and discretionary nature of the administrative actions that Plaintiffs challenge is not susceptible to review under the APA. Indeed, Plaintiffs do not identify any specific statutory standard against which OPM's information-security decisions could be judicially evaluated in a meaningful way. For example, Plaintiffs do not cite any standard by which the Court could determine whether OPM's software authorizations are sufficient, whether OPM's firewalls and host level anti-malware are adequate, or whether OPM has adequately implemented network and data segmentation. Instead, Plaintiffs ask the Court to engage in a standardless inquiry into the effectiveness of OPM's implementation of its information security program prior to the breach, immediately following the breach, and at the present time—decisions that FISMA as well as its implementing guidance recognizes must be based on a complex and technical cost-benefit, risk-based analysis. These are precisely the type of agency actions that are unreviewable because "'the courts have no legal norms pursuant to which to evaluate the challenged action, and thus no concrete limitations to impose on the agency's exercise of discretion.'" *Sierra Club*, 648 F.3d at 855 (citing *Twentymile Coal Co.*, 456 F.3d at 156). As a result, OPM's implementation of its FISMA responsibilities are "committed to agency discretion by law," and may not be reviewed under the APA. 5 U.S.C. § 701(a)(2).

---

[36] See NIST Special Publication 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations (Apr. 2013),at page vi, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

C. Plaintiffs Do Not Challenge any Discrete Agency Action Reviewable under the APA, and the APA Does Not Provide for the Broad Programmatic Relief that Plaintiffs Seek

Finally, Plaintiffs' allegations do not state an APA claim because they fail to identify a final and discrete agency action required by law that OPM failed to take and that could be remedied through a specific form of declaratory or injunctive relief. Instead, Plaintiffs seek expansive and unprecedented injunctive relief, including an order compelling OPM to comply with the Privacy Act and unspecified provisions of FISMA. But the APA does not authorize courts to enter a general order compelling compliance with broad statutory mandates, especially in data breach cases like this one. *See In re Dep't of Veterans Affairs Data Theft Litigation*, 2007 WL 7621261, at *7 (D.D.C. 2007) (dismissing with prejudice APA claim in data breach case alleging that the VA "'failed to ensure' that its 'processes, policies, and procedures were adequately implemented[,]'" because these broad allegations did "not state a challenge to discrete agency action."(citation omitted)).

The APA provides a vehicle for compelling agency action "unlawfully withheld or unreasonably delayed" and for setting aside past agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(1)-(2). However, judicial review can only proceed under these provisions if the plaintiff identifies "a discrete agency action that the agency is required to take." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64 (2004) ("*SUWA*"); *see also Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 21 (D.C. Cir. 2006) (explaining that the requirement of discrete agency action is the same regardless of whether a plaintiff challenges action taken or withheld."). Limiting judicial review to *discrete* agency action is intended

> to avoid judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve. If courts were empowered to enter general orders compelling compliance with broad statutory mandates, they would necessarily be empowered, as well, to determine whether compliance was achieved-which would

> mean that it would ultimately become the task of the supervising court, rather than the agency, to work out compliance with the broad statutory mandate, injecting the judge into day-to-day agency management. . . . The prospect of pervasive oversight by federal courts over the manner and pace of agency compliance with such congressional directives is not contemplated by the APA.

SUWA, 542 U.S. at 66-67.

Here, Plaintiffs seek sweeping and unprecedented injunctive relief. They seek to enforce, through the APA, unspecified provisions of FISMA—a very broad federal statute that provides a comprehensive framework for information security across the entire Executive branch. *See* 44 U.S.C. § 3551(1). As noted, Plaintiffs provide a laundry list of actions that OPM should have taken before and after the breach in order to comply with FISMA's requirement that it establish an adequate data security program. *See* CAC ¶¶ 82–83, 200, 202. These actions concern highly technical matters, including, for example, utilizing multi-factor authentication to access computer systems, implementing adequate network and data segmentation, and utilizing firewalls and host level anti-malware. CAC ¶ 200. However, Plaintiffs identify no statute, rule, or guidance mandating any of the actions they seek. To remedy these alleged deficiencies, Plaintiffs ask the Court to order "OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA," including by shutting down "all unauthorized information systems" until those systems are "validly authorized." *Id.* ¶ 215.

Plaintiffs' allegations do not state an APA claim because the agency actions they challenge are in no way "discrete" actions that OPM is legally required to take. Instead, Plaintiffs' allegations only suggest general deficiencies in OPM's FISMA compliance. *See*, *e.g.*, CAC ¶ 204-05 (alleging, among other things, that "OPM failed to centralize its cybersecurity governance or otherwise bring its systems into compliance"). Further, contrary to the teachings of *SUWA*, Plaintiffs' requested equitable relief clearly seeks wholesale improvement of OPM's entire information-security program,

which is not available under the APA. Plaintiffs ask the Court to order OPM "to implement a data security plan that satisfies the requirements of the Privacy Act and FISMA." CAC ¶ 215; *id.* at 75, Prayer for Relief ¶ F. This is a request to order "compliance with the broad statutory mandate" of two federal statutes; such relief is not available under the APA. *SUWA*, 542 U.S. at 66-67. Broad supervision of OPM's management of its information systems, including OPM's decisions to utilize firewalls, anti-host level malware, and data segmentation—would create "judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve" and would "inject[] the judge into day-to-day management" of OPM's information-security program. *Id.* at 66, 67. The APA does not provide for such pervasive federal-court oversight of an agency's information-security program. Plaintiffs' APA claim, therefore, should be dismissed.[37]

V. PLAINTIFFS' PARTIALLY DUPLICATIVE CLAIM FOR DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF SHOULD BE DISMISSED

In Count Four, Plaintiffs appear to allege a partially duplicative claim for what they refer to as "equitable relief." CAC ¶¶ 208-15. Specifically, Plaintiffs seek a declaration that Defendants' conduct is unlawful; a judgment requiring Defendants to indemnify Plaintiffs for all current and future economic injury as a result of the data breaches; an "injunction" requiring "free lifetime

---

[37] Plaintiffs' request under the APA for broad supervision of OPM's information-security program would not only interject the Court into the day-to-day management of information security at OPM. It would interject the Court into a host of policy matters that are currently being considered by multiple other agencies as well as the White House. On January 22, 2016, the Administration announced several major reforms to the federal background investigations process. Included in these reforms is a budget request for $95 million in additional resources to improve the IT systems which currently store background investigation data. New systems will be built, secured, and operated by the Department of Defense with the assistance of OMB and a new federal entity, the National Background Investigations Bureau (NBIB). *See* Jamal Brown, *Modernizing & Strengthening the Security & Effectiveness of Federal Background Investigations*, White House Blog (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/modernizing-strengthening-security-effectiveness-federal-background-investigations.

identity theft protection services"; and an order forcing OPM to "implement a data security plan that satisfies the requirements of the Privacy Act and FISMA." CAC ¶¶ 213-15. With respect to OPM, Plaintiffs allege that such relief is warranted under the APA, the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202 ("DJA"), and the "Court's inherent authority to order equitable remedies for unlawful actions and inactions." CAC ¶ 209. This Count fails to state a claim over which the Court has subject matter jurisdiction, or a claim upon which relief may be granted.

First, Plaintiffs' requested relief is not available under the APA because Plaintiffs lack standing to assert an APA claim and the APA does not provide relief for the claims asserted here. *See* supra Sections I and III. The APA also does not provide a vehicle for seeking money damages in the form of lifetime indemnity coverage and lifetime credit monitoring services. *See* 5 U.S.C. § 702 (waiving sovereign immunity only for actions "seeking relief other than money damages").

Second, Plaintiffs' requested relief is not available under the DJA because this statute does not provide a private right of action or an independent source of federal jurisdiction. *See*, *e.g.*, *Ali v. Rumsfeld*, 649 F.3d 762, 778 (D.C. Cir. 2011). To the extent Plaintiffs seek declaratory relief under the DJA for other claims alleged in the CAC, this request fails because Plaintiffs have not established standing or stated any claim for relief.

Finally, Plaintiffs' requested relief is not available under the Court's "inherent authority." Under the doctrine of sovereign immunity, the United States may not be sued without its consent and such consent is a requisite for jurisdiction. *United States v. Mitchell*, 463 U.S. 206, 212 (1983). The only waivers of sovereign immunity identified in the CAC are contained in the Privacy Act, the Little Tucker Act, and the APA, none of which provide relief in this case.

CONCLUSION

For all the reasons stated above, OPM's Motion to Dismiss the Consolidated Amended Complaint should be granted, and this action should be dismissed.

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director, Federal Programs Branch

/s/ Matthew A. Josephson
MATTHEW A. JOSEPHSON
ANDREW E. CARMICHAEL
KIERAN G. GOSTIN
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Room 7304
Washington, DC 20530
Tel: (202) 514-9237
Email: Matthew.A.Josephson@usdoj.gov

Dated: May 13, 2016

Counsel for Federal Defendant OPM