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: *NTEU v. Cobert*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	

FEDERAL DEFENDANT'S MEMORANDUM IN SUPPORT OF
MOTION TO DISMISS THE NTEU PLAINTIFFS' AMENDED COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

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 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.

This particular action, *National Treasury Employees Union v. Cobert* ("*NTEU*"), No. 15-cv-1808-ABJ (D.D.C. 2015), is one of over twenty civil actions filed across the United States arising from the cybersecurity incidents at OPM. The *NTEU* action is brought by NTEU on behalf of its individual members and alleges a single constitutional claim for declaratory and injunctive relief. Specifically, Plaintiffs allege that OPM had a constitutional duty to safeguard its members' personal information and that this duty was breached when a third-party cyber intruder stole their information from OPM's systems. For relief, NTEU seeks a declaration that OPM's conduct was unconstitutional, a judgment requiring OPM to provide credit-monitoring and identity-theft services to NTEU members for their entire lives, and an expansive injunction requiring OPM to take "all necessary and appropriate steps" in the future regarding its IT program and prohibiting OPM from storing NTEU members' information in electronic form.

This case should be dismissed, in its entirety, for lack of subject matter jurisdiction and for failure to state a claim upon which relief may be granted. First, Plaintiffs' constitutional claims should be dismissed because no Plaintiff can establish standing under Article III. Plaintiffs fail to establish standing for prospective relief because they allege a variety of past injuries—such as a past

fraudulent tax return, past fraudulent credit-card charges, past stolen data, and past emotional distress. Well-established standing principles hold that these past injuries are insufficient to establish standing for forward-looking equitable relief, and these injuries are not cognizable injuries in any event. Nor can Plaintiffs establish standing for declaratory and injunctive relief on the theory that at some indefinite point in the future another cyberattack could be perpetrated on OPM's systems and that this additional attack might affect the personal information of these Plaintiffs in some way. Plaintiffs' theory of future injury is entirely speculative and premised on the future actions of multiple third-party wrongdoers who are not before this Court. As such, Plaintiffs' alleged future injuries cannot establish standing.

Second, even if Plaintiffs had standing to pursue their claims, they fail to state a cognizable claim under the alleged constitutional right to informational privacy. The Supreme Court has set important limits on this assumed constitutional right that foreclose Plaintiffs' claims here. Specifically, while the Supreme Court has assumed that the Constitution might provide potential limits on the state or federal government's ability to compel the collection of certain personal information through statute or rule, the Court has never endorsed the novel idea that there is a constitutional duty to protect data from third-party theft. The Supreme Court, moreover, has made clear that the Privacy Act's statutory protections for information security are sufficient to allay any constitutional privacy concerns that might exist with respect to federal records. In addition, Plaintiffs' constitutional claim not only lacks basis in the Supreme Court's informational-privacy jurisprudence, it also conflicts with other well-established Supreme Court precedent holding that the Due Process Clause of the Fifth Amendment to the United States Constitution generally does not require the Government to affirmatively provide certain minimal levels of safety and security. Finally, Plaintiffs' constitutional claim fails because they cannot allege facts showing that OPM's

conduct "shocks the conscience"—the extremely high standard of culpability that must be met to challenge executive conduct under the substantive component of the Due Process Clause.

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

I. The Cybersecurity Incidents at OPM

This case arises from two separate but related cyber intrusions on the information technology systems and data managed by OPM. *See* NTEU Amended Complaint ¶¶ 13-19, *In Re U.S. Office of Personnel Management Data Security Breach Litig.*, No. 1:15-mc-01394-ABJ (June 3, 2016), ECF No. 75 ("NTEU Am. Compl."). The factual background of the cybersecurity incidents at OPM is presented in OPM's motion to dismiss the Consolidated Amended Complaint filed in this multidistrict litigation. ECF No. 72 ("Def.'s Mot. Dismiss CAC"). OPM incorporates that section by reference here.[1]

II. Procedural Background

A. Consolidation and Coordination through the JPML Process

This case is one of over twenty separate actions filed in numerous districts across the United States. On October 5, 2015, the U.S. Judicial Panel on Multidistrict Litigation ("JPML") granted Defendant'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

[1] Like the Plaintiffs in the Consolidated Amended Complaint, the *NTEU* Plaintiffs incorporate by reference OPM's public announcements of the cybersecurity incidents. *See* NTEU Am. Compl. ¶¶ 13-19. The announcements accordingly may be considered in resolving this motion to dismiss. *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.* ("*SAIC*"), 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)).

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 ("CAC") be filed for all transferred cases, except *NTEU v. Cobert*, 15-cv-1808-ABJ, and that the CAC will serve as the superseding, operative complaint for all plaintiffs in this MDL, except the NTEU plaintiffs. On May 13, 2016, Federal Defendant Office of Personnel Management ("OPM") moved to dismiss the claims in the CAC and in the initial complaint filed by the NTEU plaintiffs. ECF Nos. 72, 73. The NTEU plaintiffs subsequently amended their complaint. ECF No. 75. In light of the amended complaint, the Court denied, as moot, OPM's motion to dismiss the claims in the NTEU complaint and, at the request of the parties, entered a briefing schedule for filing a renewed motion to dismiss. *See* Minute Orders of May 17, 2016 and June 16, 2016.

B. The Amended Complaint in *NTEU v. Cobert*

In *NTEU v. Cobert*, [2] Plaintiff NTEU alleges a constitutional claim in its representative capacity on behalf of its members who were affected by the OPM cybersecurity incidents. NTEU Am. Compl. ¶ 5. Three individual NTEU members are named as Plaintiffs in the Amended Complaint—Eugene Gambardella, Stephen Howell, and Jonathon Ortino. *Id.* ¶¶ 6-8. The

[2] Pursuant to Federal Rule of Civil Procedure 25(d), when a public officer who is a party in an official capacity ceases to hold office, the officer's successor is automatically substituted as a party, and later proceedings should be in the substituted party's name. Accordingly, Beth F. Cobert has been substituted for her predecessor, Katherine Archuleta.

Defendant named in this case is Beth F. Cobert, Acting Director of the Office of Personnel Management, in her official capacity ("Defendant" or "OPM"). *Id.* ¶ 9.[3]

NTEU alleges that OPM violated its members' "constitutional right to informational privacy, including their right to due process under the Fifth Amendment to the U.S. Constitution." NTEU Am. Compl. ¶ 98. NTEU's constitutional theory is that OPM failed to follow the warnings of the OPM Office of Inspector General ("OIG") and the "obligations imposed on [OPM] by statute and other appropriate authority," and through these failures OPM "has manifested reckless indifference to [the] obligation to safeguard personal information provided by NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, with the assurance that it would be protected against unauthorized disclosure." *Id.* ¶ 97.

For relief, Plaintiffs seek a declaration that OPM's failure to protect their information was unconstitutional; a judgment ordering OPM to provide cost-free credit monitoring and identity-theft protection to all NTEU members for their entire lifetime; a judgment ordering OPM "to take immediately all necessary and appropriate steps to correct deficiencies in OPM's IT security program"; an injunction prohibiting OPM from "collecting or requiring the submission of NTEU members' personal information in an electronic form or storing any such information in an electronic form until the Court is satisfied that all necessary and appropriate steps" have been taken; and an award of attorney fees. *See* NTEU Am. Compl. 34-35, Request for Relief.

[3] A suit against Acting Director Cobert in her official capacity is simply another way of pleading an action against OPM itself. *See*, *e.g.*, *Hafer v. Melo*, 502 U.S. 21, 25 (1991) (citing *Kentucky v. Graham*, 473 U.S. 159, 165 (1985) ("[O]fficial-capacity suits, [in contrast,] 'generally represent only another way of pleading an action against an entity of which an officer is an agent.'"). As such, OPM refers to itself as the Defendant throughout this motion.

ARGUMENT

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

A. Plaintiffs' Alleged Past Harms And Speculative Future Harms Do Not Establish Standing To Pursue Declaratory and Prospective Injunctive Relief.

Plaintiffs exclusively seek declaratory and prospective injunctive relief in this case. *See* NTEU Am. Compl. 34-35, Request for Relief.[4] In *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983), the Supreme Court made clear that to establish Article III standing for future injunctive or declaratory relief, "past injuries alone are insufficient to establish standing"; instead, a plaintiff must demonstrate that there is a real and immediate threat that the alleged injury will be repeated in the absence of the requested injunctive relief being granted. *Dearth v. Holder*, 641 F.3d 499, 501 (D.C. Cir. 2011) (citing *Lyons*, 461 U.S. at 105); *see also Fair Emp't Council of Greater Washington, Inc. v. BMC Mktg. Corp.*, 28 F.3d 1268, 1273 (D.C. Cir. 1994) (holding that *Lyons* applies to requests for declaratory relief); *Afifi v. Lynch*, 101 F. Supp. 3d 90, 108-09 (D.D.C. 2015) (applying *Lyons*). Plaintiffs fail to establish standing under *Lyons* because the past injuries they allege are insufficient, and their allegations of future injury are entirely speculative and not redressable by their requested injunctive relief.

Here, the individual NTEU members named in the Amended Complaint allege that they have sustained four categories of past injury as a result of the OPM cybersecurity incidents: (1)

[4] Plaintiffs cannot seek money damages for their alleged constitutional claims because the United States has not waived sovereign immunity for these alleged claims and harms. *See*, *e.g.*, *Ballard v. Holinka*, 601 F. Supp. 2d 110, 121 (D.D.C. 2009) (citing *Fed. Deposit Ins. Corp. v. Meyer*, 510 U.S. 471, 477 (1994)) (explaining that the United States has not waived sovereign immunity for constitutional tort claims). In addition, a *Bivens* (*Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971)) claim for money damages, which Plaintiffs do not bring, is likewise unavailable because such a claim is precluded by the Privacy Act. *See Wilson v. Libby*, 535 F.3d 697, 709-10 (D.C. Cir. 2008); *Chung v. Dep't of Justice*, 333 F.3d 273, 274 (D.C. Cir. 2003).

Plaintiff Gambardella alleges that an unidentified third party filed a fraudulent tax return in his name and that this fraudulent return has caused him to spend time addressing the issue with the IRS, has prevented him from filing his 2015 return electronically, and has led to a delay in his tax refund, NTEU Am. Compl. ¶¶ 79-83; (2) Plaintiff Gambardella also alleges that he has experienced three fraudulent charges on an existing credit card and that these charges were resolved after contacting his credit card company, *id.* ¶ 84; (3) Plaintiffs Gambardella, Howell, and Ortino allege that they have suffered from emotional distress as a result of the OPM cybersecurity incidents, *id.* ¶ 94; and (4) Plaintiffs Gambardella, Howell, and Ortino allege that they were injured "the moment that their inherently personal information . . . was taken by unauthorized intruders from OPM's databases," *id.* ¶ 76.

None of these alleged injuries is sufficient to establish standing for declaratory and injunctive relief because all of them have already occurred—the fraudulent tax return has already been filed, the fraudulent credit card charges have already been made (and resolved), the emotional distress has already been suffered, and Plaintiffs' information has already allegedly been stolen from OPM's systems. Because all of these injuries are past injuries, they are insufficient to establish standing in this action, which involves prospective injunctive and declaratory relief only. *See, e.g.*, *Dearth*, 641 F.3d at 501.

Plaintiffs also fail to demonstrate a constitutionally adequate likelihood of future injury. In this Circuit, "[a] plaintiff must show a 'substantial probability of injury' to establish imminent injury." *Sierra Club v. Jewell*, 764 F.3d 1, 7 (D.C. Cir. 2014) (quoting *Chamber of Commerce of the U.S. v. EPA*, 642 F.3d 192, 200 (D.C. Cir. 2011)). This requirement creates "'a significantly more rigorous burden to establish standing'" than that on parties seeking redress for past injuries. *Swanson Grp. Mfg. LLC v. Jewell*, 790 F.3d 235, 240 (D.C. Cir. 2015) (citing C*hamber of Commerce v. EPA*, 642 F.3d 192, 200 (D.C. Cir. 2011)).

Accordingly, to proceed on their claims, Plaintiffs must establish that there is a substantial probability that they will suffer future injuries that will be remedied by the specific relief they have sought. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (explaining that standing is a claim- and relief- specific doctrine). In this case, Plaintiffs seek three kinds of injunctive relief: (1) an order requiring OPM to provide lifetime credit monitoring and identity theft protection to NTEU members, at no cost to those NTEU members; (2) an order requiring OPM to take immediately all necessary and appropriate steps to correct alleged deficiencies in its data security program; and (3) an order enjoining OPM from collecting or requiring the submission of NTEU members' personal information in an electronic form or storing any such information in an electronic form until the Court is satisfied those alleged deficiencies are corrected. *See* NTEU Am. Compl. 34-35, Request for Relief. Although Plaintiffs request each remedy on behalf of all NTEU members, the named Plaintiffs themselves must show a substantial probability that they will suffer a future injury that would be remedied by any of these proposed injunctions. *Sierra Club,* 764 F.3d at 6-7. Plaintiffs have not met this burden.[5]

Plaintiffs lack standing to seek the first requested injunctive remedy (requiring OPM to provide lifetime credit monitoring) because they have not established that their personal information, which was allegedly accessed during a past cyber intrusion, will be misused by a malevolent third party in the future. As such, the likelihood of this future injury occurring is based on an entirely speculative sequence of events: (1) that the individual or individuals who allegedly improperly accessed the OPM information want to commit financial malfeasance detectable by data

[5] In addition to seeking injunctive relief, Plaintiffs seek a general judgment asking the Court to declare that OPM's past conduct was unconstitutional. NTEU Am. Compl. 34, Request for Relief. To establish standing for such declaratory relief, Plaintiffs must meet the same standards established in *Lyons*. *See Fair Emp't Council of Greater Washington, Inc.*, 28 F.3d at 1273. As discussed above, Plaintiffs cannot do so.

or credit monitoring with respect to one of the named Plaintiffs; (2) that such an individual is capable of doing so; (3) that they identify and target the data of the named Plaintiffs (out of a group of approximately 22 million); (4) that such an individual actually *does* so; (5) that such an act is successful; and (6) that such an act actually causes one of the named Plaintiffs financial injury. These attenuated chains of causation do not establish Article III standing. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.* ("*In re SAIC*"), 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (rejecting claim that hypothetical future harm that is not certainly impending is enough to establish standing in data breach context); *see also Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088 (E.D. Cal. 2015) (rejecting claim that theft of information established that plaintiff "suffers from a substantial risk of imminent future harm"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954-55 (D. Nev. 2015) (same); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014) (same).[6]

Plaintiffs lack standing to seek the second requested injunctive remedy (requiring OPM to correct alleged security deficiencies) and third requested injunctive remedy (enjoining OPM from collecting Plaintiffs' personal information in electronic form) for the same reasons. Moreover, to seek these types of relief, Plaintiffs face the additional barrier of establishing that there is a substantial probability that another extraordinary cyberattack will happen in the immediate future. In an attempt to meet this requirement, Plaintiffs have alleged that their personal information, along with that of millions of others, continues to reside on OPM's systems and that OPM allegedly

[6] Plaintiffs are not entitled to seek lifetime credit monitoring for two additional reasons. First, Congress has already provided the relief Plaintiffs seek and has done so for at least the next ten years. *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, § 632, 129 Stat. 2242, 2470-71 (2015). Any future injury remediable by this Court, then, would not be until at least 2026, which does not qualify as "immediate" for purposes of establishing standing to seek prospective injunctive relief. Second, Plaintiffs have not identified a waiver of sovereign immunity that would permit them to seek this sort of monetary award. *See infra* Argument, Part III.

continues to have inadequate security measures, as evidenced by reports issued by OPM's OIG in November 2015 and May 2016 and by OPM's alleged inability to secure an able IT contractor. *See* NTEU Am. Compl. ¶¶ 87-91. But even assuming for purposes of this motion that certain inadequacies exist in OPM's systems, Plaintiffs still fail to establish that another cyber intruder will commit another extraordinary cyberattack, and that this cyberattack will injure these particular Plaintiffs—Gambardella, Howell, and Ortino—in a particular way. *See Lyons*, 461 U.S. at 101-02 (explaining that abstract injury is not enough and that "Plaintiffs must demonstrate a 'personal stake in the outcome' in order to 'assure that concrete adverseness which sharpens the presentation of issues'") (citation omitted).[7]

B. Plaintiffs Have Not Pleaded Any Cognizable Harms.

In addition to failing the *Lyons* test for standing, Plaintiffs' alleged harms are not cognizable injuries-in-fact fairly traceable to OPM's conduct. The categories of alleged harm are the same as those asserted by some Plaintiffs in the CAC and should be dismissed for the same reasons.[8]

First, Plaintiff Gambardella's allegation that a false tax return was filed in his name does not establish standing because no facts indicate that this tax fraud is fairly traceable to OPM. NTEU Am. Compl. ¶¶ 79-83. As explained in OPM's motion to dismiss the CAC, the filing of a fraudulent

[7] OPM continues to take action to strengthen its broader cyber defenses and information technology (IT) systems through efforts such as deploying two-factor strong authentication to provide a strong barrier to OPM's networks, implementing a continuous monitoring program, centralizing its IT security workforce for broader visibility across the OPM IT environment, and implementing a Data Loss Prevention System that automatically stops sensitive information, such as Social Security numbers, from leaving the network unless authorized . *See* OPM, Fact Sheet: *Cybersecurity Resource Center Frequently Asked Questions* (June, 2016), https://www.opm.gov/cybersecurity/fact-sheet.pdf. This action also reduces the possibility that another cyberattack may occur and negates the need for judicial intervention.

[8] OPM fully explained in its motion to dismiss the CAC why the categories of harms alleged by the individual NTEU members—a fraudulent tax return, fraudulent credit card charges, emotional distress, and the theft of their data—should be dismissed. It incorporates those arguments into this motion. *See* Def.'s Mot. Dismiss CAC 18-33.

tax return is a common occurrence, and it is speculative to assume that Plaintiff Gambardella's alleged injury was the result of a cyber intrusion into OPM's systems. *See* Def.'s Mot. Dismiss CAC 24. He does not allege any facts plausibly showing that the fraudulent return is connected to the information compromised in the OPM incidents, that the intruders responsible for the cybersecurity incidents at OPM are also filers of a fraudulent tax return allegedly filed in his name, or that the intruders shared or sold particular categories of information to an individual or individuals who would likely file a fraudulent return.

Instead, Plaintiff's sole allegation intended to suggest that the filing of a fraudulent tax return in his name was a result of the alleged OPM cyber incident is his assertion that "to the best of his knowledge" he has not "had his personal information exposed in any other public or private sector data breach" and has not "been the victim of identity theft other than the instances described in this amended complaint." NTEU Am. Compl. ¶ 82. But the fact that Gambardella is not aware of any other data breaches or identity-theft incidents affecting his information does not show that such a breach or incident has not occurred, let alone plausibly demonstrate that it was OPM's conduct (as opposed to the conduct of some third party) that caused the filing of the fraudulent tax return. To the contrary, Plaintiff Gambardella's allegations of tax fraud rest entirely on speculation about the actions of third-party wrongdoers—namely, the individual or individuals who committed the tax fraud—and therefore 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 v. U.S. Dep't of Interior*, 563 F.3d 466, 478 (D.C. Cir. 2009) (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.").

Second, Plaintiff Gambardella cannot establish standing by alleging that he has sustained three instances of fraudulent financial charges on his existing credit card. 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* Def.'s Mot. Dismiss CAC 19-20 (citing *Whalen v. Michael Stores Inc.*, No. 14-cv-7006, 2015 WL 9462108, at *3 (E.D.N.Y. Dec. 28, 2015); *Hammond v. The Bank of New York Mellon Corp.*, No. 08-cv-6060, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at*6 (N.D. Ill. Sept. 3, 2013); *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1280–81 (N.D. Ala. 2014)). Here, Plaintiff Gambardella specifically recognizes that the fraudulent charges were resolved after contacting his credit card company. NTEU Am. Compl. ¶ 84. Mr. Gambardella's allegations of financial fraud, accordingly, cannot establish standing.

In addition, Plaintiff Gambardella's alleged instances of financial fraud do not establish standing because no facts plausibly show that this financial fraud is fairly traceable to OPM's conduct. As OPM explained in its motion to dismiss the CAC, and as explained in summary fashion here:

> (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 that Plaintiff Gambardella alleges is particular to him, varies from the financial fraud alleged by other plaintiffs in this multidistrict litigation (including the other two NTEU members who do not even allege any financial fraud), and thus do not suggest that the fraud is causally connected to one data breach, let alone the OPM incidents;
>
> (3) Plaintiff Gambardella's allegations of existing-account fraud are especially deficient because no facts indicate that the credit card number that was allegedly misused was stolen during the OPM

> cybersecurity incidents, and Plaintiff does not specifically state facts indicating how a criminal could have obtained a particular financial account number by using information that was stolen.

See Def.'s Mot. Dismiss CAC 19-26. In these circumstances, it cannot plausibly be assumed that OPM's conduct caused the fraudulent financial charges that were made on his account.

Third, Plaintiffs Gambardella, Howell, and Ortino cannot establish standing by alleging that they have suffered emotional distress as a result of the OPM cybersecurity incidents. *See* Def's Mot. Dismiss CAC 31-33. 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 v. Ceridian Corp.*, 664 F.3d 38, 44-46 (3d Cir. 2011); *Low v. LinkedIn Corp.*, No. 11-cv-1468, 2011 WL 5509848, at *3-*4 (N.D. Cal. Nov. 11, 2011). Here, Plaintiffs Gambardella, Howell, and Ortino do not allege any facts showing that they personally face an imminent injury as a result of the incidents. Rather their alleged "emotional distress and anxiety" is based on the unspecified future "effect that these data breaches will have on them, their families, and other associates." NTEU Am. Compl. ¶ 94. Thus, their alleged emotional distress is not a cognizable injury under Article III.

Finally, Plaintiffs Gambardella, Howell, and Ortino cannot establish standing by alleging that they were injured "the moment that their inherently personal information . . . was taken by unauthorized intruders from OPM's databases." NTEU Am. Compl. ¶ 76. The clear majority of federal courts, including this court, have concluded that "the mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing." *In re SAIC*, 45 F. Supp. 3d at 19; *see also In re SuperValu, Inc.*, No. 14-MD-2586, 2016 WL 81792, at *4 (D. Minn. Jan. 7, 2016) ("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.") (collecting cases). Indeed, the Supreme Court recently emphasized that only concrete injuries are sufficient to establish standing. *See generally Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). The alleged theft of personal information—untethered from any real, de-facto harm—is exactly the type of abstract harm that is too nebulous to satisfy that requirement. *See id.* at 1550 (noting that the incorrect reporting of a plaintiff's zip code by a consumer reporting agency would not be sufficient to establish standing).

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

In addition to the claims asserted by individual Plaintiffs Gambardella, Howell and Ortino, Plaintiff NTEU seeks to assert claims "in its representative capacity on behalf of its members who have been injured by the Defendant's failure to protect their personal information." NTEU Am. Compl. ¶ 5. NTEU cannot establish standing to do so, however. 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. EPA.*, 667 F.3d 6, 12 (D.C. Cir. 2011). As such, plaintiff-organizations must "make *specific allegations* establishing that at least one identified member had suffered or would suffer harm." *Summers v. Earth Island Inst.*, 555 U.S. 488, 498 (2009) (emphasis added); s*ee also Am. Chemistry Council v. Dep't of Transp.*, 468 F.3d 810, 820 (D.C. Cir. 2006). As explained, the only individual NTEU members identified in the Complaint are Plaintiffs Gambardella, Howell and Ortino, and they cannot establish standing to assert their individual claims. The failure of any individual Plaintiff to establish standing is fatal to NTEU's representational standing in this case.

II. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE CONSTITUTIONAL RIGHT TO INFORMATIONAL PRIVACY.

Even if Plaintiffs could establish standing, their constitutional claims still should be dismissed for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6) because the Due

Process Clause of the Fifth Amendment does not impose a duty on the government to protect information from third-party theft.

NTEU alleges that a third-party's theft of their personal information from OPM's systems violated their "constitutional right to informational privacy, including their right to Due Process under the Fifth Amendment to the U.S. Constitution." NTEU Am. Compl. ¶ 98; *see also id.* ¶¶ 95-98. Plaintiffs allege that OPM had a constitutional "duty to safeguard NTEU members' personal information," *id.* ¶ 96, and that this duty was violated because OPM "has manifested reckless indifference to [its] obligation to safeguard personal information provided by NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, with the assurance that it would be protected against unauthorized disclosure." *Id.* ¶ 97. Plaintiffs' allegations do not state a cognizable constitutional claim and should be dismissed.[9]

A. Precedent From The Supreme Court And The D.C. Circuit Addressing The Constitutional Right To Informational Privacy Does Not Support Plaintiffs' Claim In This Case.

In a trio of cases, the Supreme Court has assumed that the Constitution protects the individual "interest in avoiding disclosure of personal matters" and accordingly has considered whether the Constitution might impose some limit on the amount or type of information that the government may collect from private citizens. *See Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 138 (2011); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457 (1977). The Court, however, has not specifically held that this constitutional privacy right, often referred to as the constitutional right to informational privacy, actually exists, nor has the Court explained the nature of such a right or its textual source. Instead, the Court has "assume[d],

[9] Plaintiffs also allege that the information stolen from OPM's databases is subject to the Privacy Act, 5 U.S.C. § 552a, *see* NTEU Am. Compl., ¶¶ 67-69, although unlike all other Plaintiffs in this MDL, they do not allege any claim under the Privacy Act.

without deciding, that the Constitution protects a privacy right of [this] sort" before finding that the Government's actions did not violate the assumed right in the case at hand. *See Nelson*, 562 U.S. at 138; *Whalen*, 429 U.S. at 605-06; *Nixon*, 433 U.S. at 457-65.[10]

The D.C. Circuit also has never specifically held that the constitutional right to informational privacy exists and has expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997). Nonetheless, following the Supreme Court's approach, the Circuit has assumed, without deciding, that such a right might exist before concluding that the Government's actions did not violate the assumed right under the specific facts of the case. *See id.* at 793.[11]

Without any definitive guidance from the Supreme Court or the D.C. Circuit, the existence of the right to informational privacy remains unclear. Nevertheless, the Court need not resolve that issue in this particular case to conclude that Plaintiffs' allegations do not state a cognizable constitutional claim. The cases addressing the constitutional right to privacy contain important limits that do not support the novel contention that the Constitution imposes a duty to protect personal data—already subject to the Privacy Act's protections—from third-party theft. Notably, in all three cases in which the Supreme Court has assumed that the constitutional right to informational

[10] Several justices have criticized that approach and questioned the very existence of a constitutional right to informational privacy. *See Nelson*, 562 U.S. at 159-60 (Scalia, J., concurring in the judgment) ("'[I]nformational privacy' seems like a good idea…[b]ut it is up to the People to enact those laws, to shape them, and, when they think it appropriate, to repeal them. A federal constitutional right to 'informational privacy' does not exist."); *id.* at 169 (Thomas, J., concurring in the judgment) ("I agree with Justice Scalia that the Constitution does not protect a right to informational privacy. No provision in the Constitution mentions such a right." (internal citations omitted))).

[11] "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) (citation omitted); *see also Murphy v. F.D.I.C.*, 208 F.3d 959, 965-66 (11th Cir. 2000) (same).

privacy might exist, it considered only whether this assumed right could provide potential limits on the state or federal government's ability to compel the collection of certain personal information, either through passage of a state or federal statute or an agency rule. The Court also has explained in these cases that the presence of statutory or regulatory protections against unauthorized disclosure by the government – specifically the protections in the Privacy Act – generally allay any privacy concerns that might arguably have constitutional roots.

The Supreme Court first addressed the constitutional right to informational privacy in *Whalen v. Roe*, 429 U.S. 589 (1977). In *Whalen*, the Court considered a privacy-based constitutional challenge to a New York statute requiring physicians and pharmacists to report prescription information for certain narcotics to the state health department. *Id.* at 591, 593. The state agency collected that information in order to identify stolen or altered prescriptions and uncover abuse of prescription narcotics. *Id.* at 593. A group of patients who regularly received drugs subject to the reporting requirements claimed the statute violated their constitutional right to privacy, arguing that the compelled disclosure of their information to the state could lead to the information being publicly disclosed, *id.* at 600, and that fear of possible public disclosure might cause some patients to decline medically necessary prescriptions. *Id.*

The Supreme Court rejected the notion that required disclosure to public health agencies or other bodies charged with the public welfare violated the Constitution. *Id.* at 603. The Court acknowledged that the disclosure of "private information" to the State could be an "unpleasant invasion[] of privacy," *id.* at 602, but the Court pointed out that the New York statute's provisions and implementing administrative procedures protected against "[p]ublic disclosure" of patients' information, *id.* at 600–01. This sort of "statutory or regulatory duty to avoid unwarranted disclosures" of "accumulated private data" was sufficient, in the Court's view, to protect a privacy interest that "arguably ha[d] its roots in the Constitution." *Id.* at 605–06. The Court accordingly

held that the New York statute requiring patients to disclose medical information to the state does not violate any right to privacy that might exist in the Constitution. *Id.*

Several months after *Whalen* was decided, the Court issued its second decision addressing the constitutional right to informational privacy. In *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977), the Court rejected a facial constitutional challenge to provisions of a federal statute—the Presidential Recordings and Materials Preservation Act, 44 U.S.C. § 2111—that compelled President Nixon to turn over his Presidential papers and tape-recorded conversations for archival review and screening. 435 U.S. at 429. President Nixon contended that it would violate his constitutional right to privacy to allow government archivists to review his papers to determine which ones concerned official business (and therefore would be archived) and which concerned personal matters (and would be returned to him). *Id.* at 434, 454-55, 459. The Court rejected those challenges and concluded that the compelled review of private materials contemplated by the statute was constitutionally permissible. As pertinent here, the Court explained that the informational privacy claim "cannot be considered in the abstract" and instead "must be considered in light of the specific provisions of the Act[.]" *Id.* at 458. As in *Whalen*, the Court emphasized that the statute at issue "mandate[d] regulations . . . aimed at preventing undue dissemination of private materials[.]" *Nixon*, 433 U.S. at 458. The Court accordingly upheld the constitutionality of the federal Act at issue.

Most recently, in *National Aeronautics and Space Administration v. Nelson*, 562 U.S. 134 (2011), the Court addressed a privacy-based constitutional challenge to the Government's use of mandatory questionnaires, known as Standard Form ("SF") 85 and Form 42, during the background-investigation process for employment under a federal contract. *Id.* at 134-35. These questionnaires required employees and federal contractors to disclose information regarding their prior illegal drug use and rehabilitation, and required the employee's or contractor's self-designated references to answer questions regarding the employee's trustworthiness, honesty, and suitability for federal

employment. *Id.* The Court assumed, without deciding, that such inquiries implicated the *Whalen* and *Nixon* interest in avoiding disclosure of personal information. *Id.* at 147-48. The Court ultimately determined, however, that the background-check questions were reasonable employment-related inquiries and thus did not violate an assumed constitutional right to informational privacy. *See id.* at 157-58. In reaching this conclusion, the Court emphasized that the information on SF-85 and Form 42 are "subject to substantial protections against disclosure to the public." *Id.* at 155. Citing *Whalen* and *Nixon*, the Court explained that, while "government 'accumulation' of 'personal information' for 'public purposes' may pose a threat to privacy," these privacy concerns are generally allayed by a "statutory or regulatory duty to avoid unwarranted disclosures." *Nelson*, 562 U.S. at 155 (citing *Whalen*, 429 U.S. at 605 and *Nixon*, 433 U.S. at 458-59). The Court specifically noted that the Privacy Act covered all the information at issue in the challenged forms and provided numerous protections against unwarranted public disclosure. *Id.* (citing 5 U.S.C. §§ 552a(e)(1), 552a(b), 552a(i)(1)). These statutory provisions, the Court explained, "evidence a proper concern" for individual privacy. *Id.* at 156 (citing *Whalen*, 429 U.S. at 605 and *Nixon*, 433 U.S. at 458-59). In rejecting plaintiffs' constitutional claim, the Court also emphasized the nature of the employee-employer relationship, noting that "the Government has a much freer hand in dealing 'with citizen employees than it does when it brings its sovereign power to bear on citizens at large.'" *Id.* at 148 (citation omitted).

Whalen, *Nixon*, and *Nelson* set important limits on any informational privacy right that foreclose Plaintiffs' claim here. First and most fundamentally, in all three decisions, the Supreme Court assumed that the constitutional right to informational privacy could provide potential limits on the state or federal government's ability to compel *the collection* of certain personal information, either through passage of a state statute (*Whalen*), a federal statute (*Nixon*), or agency rule implementing a presidential directive (*Nelson*). Plaintiffs, however, do not challenge OPM's

collection of their information pursuant to legal authority—and indeed, such a claim clearly would be foreclosed by *Nelson*. To be sure, unlike the plaintiffs in *Whalen*, *Nixon*, and *Nelson*, Plaintiffs here do not challenge any particular statute, regulation, or rule requiring an individual to disclose a particular category of personal information to the government. Instead, Plaintiffs contend that Defendant has a constitutional duty to protect personal information in its possession from third-party theft. NTEU Am. Compl. ¶¶ 96-98. But the informational-privacy cases establish no such duty. Because this case does not concern any challenge to the government's collection of information pursuant to legal authority, *Whalen*, *Nixon*, and *Nelson* do not support Plaintiffs' informational privacy claims here.[12]

Second, the informational-privacy cases make clear that the presence of statutory or regulatory protections against unauthorized disclosure by the government generally allay any privacy concerns that might arguably have constitutional roots. *See Nelson*, 562 U.S. at 155 (citing *Whalen*,

[12] The handful of cases in the D.C. Circuit squarely addressing the assumed constitutional right to informational privacy likewise provide no support for Plaintiffs' claims. In all of these cases, the Circuit addressed whether the Government's collection of information, pursuant to a particular statute or rule, was consistent with the assumed constitutional right to informational privacy. *See*, *e.g.*, *Am. Fed'n of Gov't Emps.*, 118 F.3d at 795 (holding that questionnaires and release forms used by the Department of Housing and Urban Development and the Department of Defense to collect information about employees' finances and illegal drug use were constitutionally permissible); *United Steelworkers of Am., AFL-CIO-CLC v. Marshall*, 647 F.2d 1189, 1240-41 (D.C. Cir. 1980) (rejecting plaintiff union's contention that rules implementing the Occupational Safety and Health Act granting access to employee medical records to both government agencies and authorized representatives violated employees' constitutional right to privacy); *Franklin v. Dist. of Columbia*, 163 F.3d 625, 638-39 (D.C. Cir. 1998) ("For these reasons, we hold that Spanish-speaking prisoners with limited proficiency in English do not have a privacy right, derived from the Constitution, to force the District to hire bilingual medical personnel so that the prisoners may communicate their medical information only to such employees."); *id.* at 638 ("[W]hen recognized in the past, the constitutional right of privacy has protected against disclosure to the state." (citing *Whalen*, 429 U.S. at 599); *Nat'l Fed'n of Fed. Emps. v. Greenberg*, 983 F.2d 286, 294-95 (D.C. Cir. 1993) (holding that Department of Defense's use of security questionnaire gathering information on, among other subjects, an employee's drug use did not violate assumed constitutional right to privacy). No case from the D.C. Circuit supports recognizing Plaintiffs' constitutional claim here, which does not challenge the Government's ability to collect information from an individual but instead seeks to impose a constitutional duty to protect an individual's information from misuse by a third party.

429 U.S. at 605 and *Nixon*, 433 U.S. at 458-59). Specifically, in *Nelson*, the Supreme Court explained that the Privacy Act's comprehensive requirements "give 'forceful recognition' to a Government employee's interest in maintaining the 'confidentiality of sensitive information . . . in his personnel files," *Nelson*, 562 U.S. at 156 (alterations in original) (citing *Detroit Edison Co. v. NLRB*, 440 U.S. 301, 318 n.16 (1979)), and "'evidence a proper concern' for individual privacy," *id.* (citations omitted). Notably, the Court explained that the Privacy Act's protections are sufficient to satisfy any constitutional privacy concerns even if an individual's information is affected by a data breach at a federal agency. The Court recognized that "data breaches are a possibility any time the Government stores information" and "the mere possibility that security measures will fail provides no 'proper ground' for a broad-based attack on government information-collection practices." *Nelson*, 562 U.S. at 158 (citing *Whalen*, 429 U.S. at 601–02). The Court also explained that the Privacy Act is sufficient to allay any constitutional concerns even if a Plaintiff might not be able to sue the United States for damages or injunctive relief. *Id.* at 158-59 n.15 ("Nothing in *Whalen* or *Nixon* suggests that any private right of action—for money damages or injunctive relief—is needed in order to provide sufficient protection against public disclosure."); *see also Wilson v. Libby*, 535 F.3d 697, 709 (D.C. Cir. 2008) (explaining that the Privacy Act provides a comprehensive scheme precluding a constitutional privacy claim for money damages under *Bivens*, even if the Privacy Act does not provide "a remedy to the particular plaintiff for the particular claim he or she wishes to pursue.").

Finally, as the Supreme Court reiterated in *Nelson*, a proper analysis of any constitutional right to informational privacy must account for the fact that "the Government has a much freer hand in dealing 'with citizen employees than it does when it brings its sovereign power to bear on citizens at large.'" *Nelson*, 562 U.S. at 148 (citation omitted). Here, when the Government makes decisions concerning the management and security of data, "it does not exercise its sovereign power 'to regulate or license.'" *Id.* at 148 (citation omitted). Instead, the Government conducts its

information security program "as proprietor" and manager of its "internal operation." *Id.* (citation omitted). Any assessment of the constitutionality of OPM's information-security practices must account for this distinction, which does not support Plaintiffs' request to constitutionalize OPM's information-security policies.

In sum, the Supreme Court's decisions addressing the assumed constitutional right to informational privacy do not support the novel contention that the Constitution imposes a duty to protect personal data—already subject to the Privacy Act's protections—from third-party theft. Plaintiffs, therefore, fail to state a cognizable constitutional claim.

B. The Fifth Amendment Does Not Impose An Affirmative Constitutional Duty On The Federal Government To Protect Data From Theft By Third Parties.

Plaintiffs' theory that the Constitution imposes a duty upon the government to protect their data from third-party theft not only lacks support in the informational privacy cases but also directly conflicts with other well-established Supreme Court precedent interpreting the substantive component of the Due Process Clause.

As an initial matter, the Supreme Court has "always been reluctant to expand the concept of substantive due process because guideposts for responsible decisionmaking in this unchartered area are scarce and open-ended." *Collins v. City of Harker Heights*, 503 U.S. 115, 125 (1992) (citing *Regents of Univ. of Mich. v. Ewing*, 474 U.S. 214, 225-26 (1985)). It is therefore important, the Court explained, "to focus on the allegations in the complaint to determine how [a plaintiff] describes the constitutional right at stake and what the [government] allegedly did to deprive [the plaintiff] . . . of that right." *Estate of Phillips v. Dist. of Columbia*, 455 F.3d 397, 403 (D.C. Cir. 2006) (citing *Collins*, 503 U.S. at 125); *see also Washington v. Glucksberg*, 521 U.S. 702, 721 (1997) (explaining that the Court "[has] required in substantive-due-process cases a 'careful description' of the asserted fundamental liberty interest." (citation omitted)).

More specifically, in *DeShaney v. Winnebago County Department of Social Services*, 489 U.S. 189 (1989), the Supreme Court made clear that the Due Process Clauses of the Fifth and Fourteenth Amendments to the United States Constitution "generally confer no affirmative right to governmental aid, even where such aid may be necessary to secure life, liberty, or property interests of which the government itself may not deprive the individual." *Id.* at 196. In that case, a four-year-old child, Joshua DeShaney, was beaten and permanently injured by his father, with whom he lived and about whom county social workers had received several abuse complaints. *Id.* at 191. Despite the fact that county officials "had reason to believe" that the abuse was ongoing and despite the fact that they "did not act to remove [Joshua] from his father's custody," *id.*, the Court held that the County's actions did not violate the Due Process Clause. "[N]othing in the language of the Due Process Clause itself," the Court reasoned, "requires the State to protect the life, liberty, and property of its citizens against invasion by private actors," because "[t]he Clause is phrased as a limitation on the State's power to act, not as a guarantee of certain minimal levels of safety and security." *Id.* at 195; *see also Collins*, 503 U.S. at 126 ("Neither the text nor the history of the Due Process Clause supports petitioner's claim that the governmental employer's duty to provide its employees with a safe working environment is a substantive component of the Due Process Clause.").

Here, NTEU alleges that Defendant violated its members' purported constitutional right to informational privacy by failing to protect their personal information from theft by a third-party intruder. NTEU Am. Compl. ¶¶ 95-98; *see also* ¶¶ 13-19. But *DeShaney* makes clear that the Due Process Clause does not require the State to affirmatively protect an individual from harm by third-party actors. *DeShaney*, 489 U.S. at 195. Further, if the State is not constitutionally required to protect the *life* of an individual from physical violence by third parties, then, *a fortiori*, there is no

constitutional basis for imposing a duty to protect an individual's data or information from a third-party cyber intruder.

It is true that the Supreme Court has recognized limited exceptions to the general rule that the Constitution does not impose affirmative duties of care and protection with respect to particular individuals. But those exceptions do not apply here. Specifically, "when the State takes a person into its custody and holds him there against his will, the Constitution imposes upon it a corresponding duty to assume some responsibility for his safety and general well-being." *Id.* at 199-200 (citation omitted). The theory behind this exception is simple:

> [W]hen the State by the affirmative exercise of its power so restrains an individual's liberty that it renders him unable to care for himself, and at the same time fails to provide for his basic human needs—*e.g.,* food, clothing, shelter, medical care, and reasonable safety—it transgresses the substantive limits on state action set by the Eighth Amendment and the Due Process Clause. . . .[I]t is the State's affirmative act of restraining the individual's freedom to act on his own behalf—through incarceration, institutionalization, or other similar restraint of personal liberty—which is the 'deprivation of liberty' triggering the protections of the Due Process Clause, not its failure to act to protect his liberty interests against harms inflicted by other means.

Id. at 200 (citation omitted).

The D.C. Circuit has applied this *Dehsaney* exception narrowly, holding that it only applies when there is physical confinement of the injured party, including through incarceration or institutionalization. In this custodial context, "special circumstances" of a "special relationship" may arise between the State and the individual such that the State has an affirmative duty to protect the individual. *See Estate of Phillips*, 455 F.3d at 406 (explaining that a Due Process claim premised on the failure to act must involve the "special circumstances" of a "special relationship" in which an individual's physical liberty is restrained); *Fraternal Order of Police Dep't of Corr. Labor Comm. v. Williams*, 375 F.3d 1141, 1146 (D.C. Cir. 2004) (explaining that, under *Deshaney*, a Due Process violation must be premised on "special circumstances" like physical "custody" which might give rise to an

affirmative duty to protect); *Richmond v. Potter*, No. 03-cv-00018-CKK, 2004 WL 5366540, at *9 (D.D.C. Sept. 30, 2004) ("[T]he vast majority of caselaw stands for the proposition that—without custody—such 'special circumstances' [necessary for a Due Process violation] do not exist.") (collecting cases), *aff'd*, 171 F. App'x 851 (D.C. Cir. 2005).

Here, Plaintiffs' Due Process Claim fails because they do not identify any "special relationship" or state-imposed restraint on their liberty that could give rise to a Due Process violation. To be sure, this case does not involve physical custody at all but rather the custody of data. This case, moreover, involves an employment relationship between the federal government and current and former federal employees. NTEU Am. Compl. ¶¶ 5-8. In the public employment context, the D.C. Circuit has "consistently rejected imposing a heightened employer-to-employee obligation because of the absence of a state-imposed restraint on liberty." *Estate of Phillips*, 455 F.3d at 406. Thus, because this case does not involve any state-imposed restraint on liberty, Plaintiffs' informational privacy claim, premised on the Due Process Clause, fails to state a cognizable constitutional claim.

C. Plaintiffs Fail To Allege Facts Showing That OPM's Conduct "Shocks The Conscience."

As explained above, Plaintiffs' informational privacy claim under the Fifth Amendment fails to state a claim because this case does not involve any "special relationship" or state-imposed restraint on liberty that could give rise to a Due Process violation. *See Estate of Phillips*, 455 F.3d at 406; *Williams*, 375 F.3d at 1146. Nonetheless, even if one were to overlook the fact that this case does not involve any kind of physical custody, Plaintiffs still fail to state a claim under the Fifth Amendment because they do not allege facts that shock the conscience.

To state a substantive due process violation based on executive conduct, a plaintiff must plead facts showing that the government's alleged conduct "was so egregious, so outrageous, that it may fairly be said to shock the contemporary conscience." *Williams*, 375 F.3d at 1144-45 (citation

omitted); *see also Cty. of Sacramento v. Lewis,* 523 U.S. 833, 847 n.8 (1998). The conscience-shock inquiry is a "stringent requirement" that "exists to differentiate substantive due process . . . from local tort law." *Williams*, 375 F.3d at 1145 (alteration in original) (citation omitted). The stringent requirement of "conscience-shocking" behavior may be met by two levels of government behavior. First, behavior most likely to support a due process claim is intentional "conduct intended to injure in some way unjustifiable by any government interest." *Lewis*, 523 U.S. at 849, 854. Second, the Supreme Court has instructed that, in certain situations, "deliberate indifference can rise to a constitutionally shocking level." *Id.* at 852. In evaluating whether executive action shocks the conscience, the Supreme Court has recognized the "presumption that the administration of government programs" and "[d]ecisions concerning the allocation of resources" are "based on a rational decisionmaking process that takes account of competing social, political, and economic forces." *Williams*, 375 F.3d at 1145 (citing *Collins,* 503 U.S. at 128). As a result, "large-scale personnel and program decisions" made by government officials are not the sort of government conduct likely to rise to the conscience-shocking level. *See Williams*, 375 F.3d at 1145 (citing *Lewis,* 523 U.S. at 849); *see also Collins,* 503 U.S. at 129 ("The Due Process Clause 'is not a guarantee against incorrect or ill-advised personnel decisions.'" (citation omitted)).

Here, NTEU certainly does not allege that OPM engaged in any intentional conduct designed to injure its members. Instead, Plaintiffs allege that Defendant has "manifested reckless indifference to her obligation to safeguard personal information provided by NTEU members . . . ." NTEU Am. Compl. ¶ 97; see also *id.* ¶¶ 58, 75, 77, 78, 92-94. Specifically, NTEU alleges that the OPM OIG conducted a required audit under the Federal Information Security Management Act ("FISMA"), and concluded that OPM was not in compliance with certain information-security rules and standards. NTEU Am. Compl. ¶¶ 36-57. The alleged noncompliance includes deficiencies related to OPM's "decentralized security governance," *id.* ¶ 44; the fact that a comprehensive

assessment was not completed on time for 11 of 21 OPM systems, *id.* ¶¶ 45-46; that "OPM needs to improve its technical security controls relate[d] to configuration management and authentication of IT systems using personal identity verification (PIV) credentials," *id.* ¶¶ 47-48, 50; and that OPM does not maintain "an accurate centralized inventory of all servers and data bases that reside within the network," *id.* ¶ 49. But such alleged deficiencies in a federal agency's information-security program come nowhere close to approaching conduct that shocks the conscience. OPM's information-security decisions are precisely the type of "large-scale personnel and program decisions" made by government officials that do not rise to the conscience-shocking level. *Williams*, 375 F.3d at 1145 (citing *Lewis*, 523 U.S. at 849); *see also Collins* 503 U.S. at 128-29 ("Decisions concerning the allocation of resources to individual programs, . . . involve a host of policy choices that must be made by locally elected representatives, rather than by federal judges interpreting the basic charter of Government for the entire country."). In sum, Plaintiffs' allegations that OPM did not adequately implement its information-security responsibilities do not rise to levels that shock the conscience. Plaintiffs, therefore, cannot state an informational privacy claim premised on the Due Process Clause.

III. PLAINTIFFS' REQUEST FOR RELIEF IN THE FORM OF LIFETIME CREDIT MONITORING SERVICES IS BARRED BY SOVEREIGN IMMUNITY.

Because Plaintiffs fail to establish standing and fail to state a cognizable constitutional claim, the Court need not address the propriety of their requested remedies. *See* NTEU Am. Compl. 34-35, Request for Relief. Nonetheless, NTEU's request for relief in the form of lifetime credit monitoring services is barred by sovereign immunity. *Id.* ¶ B. To state a claim against the United States, Plaintiffs must identify a clear waiver of sovereign immunity for the claim alleged and remedy sought. *See*, *e.g.*, *United States v. White Mountain Apache Tribe*, 537 U.S. 465, 472 (2003). Here, Plaintiffs do not identify any statute that would waive sovereign immunity for the payment of

lifetime credit monitoring services, which at a minimum would cost well over a hundred million dollars. *See* News Release, *OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract*, U.S. Office of Personnel Management (September 1, 2015), https://www.opm.gov/news/releases/2015/09/opm-dod-announce-identity-theft-protection-and-credit-monitoring-contract (explaining that three years of credit monitoring services alone cost $133 million).

CONCLUSION

For all the reasons stated above, the *NTEU* action should be dismissed pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6).

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
JOSEPH E. BORSON
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: June 27, 2016

***Counsel for Federal Defendant* OPM**