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 REPLY MEMORANDUM IN SUPPORT OF MOTION TO DISMISS THE NTEU PLAINTIFFS' AMENDED COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

PRELIMINARY STATEMENT

Plaintiff National Treasury Employees Union ("NTEU") and three of its federal-employee members allege a single constitutional claim for declaratory and injunctive relief in this case arising out of the cybersecurity incidents at the Office of Personnel Management ("OPM"). Plaintiffs allege that OPM has a constitutional duty under the Fifth Amendment to the United States Constitution to protect Plaintiffs' data from third-party cyber intruders, and further allege that this constitutional duty was breached when a third-party intruder stole Plaintiffs' information from OPM's systems in a malicious and sophisticated manner. This case should be dismissed because Plaintiffs cannot overcome their failure to establish standing under Article III to pursue injunctive relief for their constitutional claim. In addition, even if Plaintiffs could establish standing, they fail to state a valid claim under the Fifth Amendment.

Plaintiffs' constitutional claim should be dismissed because none of the Plaintiffs can establish standing under Article III. Black-letter law holds that past injuries are insufficient to establish standing for declaratory and prospective injunctive relief—the only form of relief at issue in this case. Yet, Plaintiffs continue to rely in their opposition on a variety of past injuries to establish standing, such as a past fraudulent tax return, past fraudulent credit-card charges, past stolen data, and past emotional distress. Plaintiffs also make no showing in their opposition that they face a substantial risk of imminent future injury that would be redressed by their requested injunction. Plaintiffs' theory of future injury is that, at some indefinite point in the future, another cyber intruder might commit another cyberattack on OPM's systems resulting in unauthorized access to information and that this attack might affect the personal information of Plaintiffs in some way. But 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. Plaintiffs' alleged future injuries cannot establish standing.

Even if Plaintiffs had standing to pursue their claims, they fail to state a cognizable claim under the alleged constitutional right to informational privacy. Plaintiffs allege that OPM violated the Due Process Clause of the Fifth Amendment because OPM failed to protect Plaintiffs' data from theft by third-party cyber intruders. But the Due Process Clause does not impose any general affirmative duty to protect individuals from third-party harm. Instead, as Plaintiffs acknowledge in their opposition, an affirmative constitutional duty to protect against third-party harm only arises in exceptional circumstances, such as when the government has physically imprisoned an individual and therefore made it impossible for that individual to meet his or her basic human needs. Those circumstances are not present here. And contrary to Plaintiffs' contention, the government's custody of information is not analogous to imprisoning an individual. Retaining custody of information does not restrict an individuals' physical liberty to act on their own behalf, and thus does not trigger any affirmative constitutional duty of care under the Due Process Clause. Finally, Plaintiffs' constitutional claim also fails because large-scale personnel and program decisions—like OPM's decisions regarding its information security program—are not the type of government actions that shock the contemporary conscience, the extremely high level of culpability that must be met to state a substantive due process claim challenging executive conduct under the Fifth Amendment.

ARGUMENT

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

A. Plaintiffs' Alleged Past Injuries Fail To Establish Standing To Pursue Declaratory And Prospective Injunctive Relief.

Plaintiffs exclusively seek declaratory and injunctive relief, which is the only possible form of relief for the constitutional claim they allege. *See* NTEU Mem. Opp'n OPM Mot. Dismiss Am. Compl. ("NTEU Mem.") 22-24 (ECF No. 84); *see also* NTEU Am. Compl. ¶¶ 34-35, Request for

Relief (ECF No. 75).[1] "[W]here the plaintiffs seek declaratory and injunctive relief, past injuries alone are insufficient to establish standing." *Dearth v. Holder*, 641 F.3d 499, 501 (D.C. Cir. 2011); *see also City of Los Angeles v. Lyons*, 461 U.S. 95, 106 (1983). Instead, when declaratory and injunctive relief is sought, a plaintiff "must show he is suffering an ongoing injury or faces an immediate threat of future injury." *Afifi v. Lynch*, 101 F. Supp. 3d 90, 108 (D.D.C. 2015) (citing *Lyons*, 461 U.S. at 105).

Plaintiffs confirm in their opposition that they are relying on four categories of alleged past injury as the result of the OPM cybersecurity incidents: (1) Plaintiff Gambardella alleges that an unidentified third party filed a fraudulent tax return in his name in the past; NTEU Mem. 15, NTEU Am. Compl. ¶¶ 79-83; (2) Plaintiff Gambardella also alleges that he experienced three fraudulent charges on an existing credit card (which were resolved by the credit card company) in the past; NTEU Mem. 15, NTEU Am. Compl. ¶ 84; (3) Plaintiffs Gambardella, Howell, and Ortino allege that they suffered in the past emotional distress as a result of the OPM cybersecurity incidents, NTEU Mem. 18, NTEU Am. Compl. ¶ 94; and (4) Plaintiffs Gambardella, Howell, and Ortino allege that they were injured, in the past, "the moment their data was taken from OPM's databases," NTEU Mem. 8-11, 20, NTEU Am. Compl. ¶ 76.

Putting aside whether any of these four categories of past injuries could establish standing to seek money damages for past harm (which is not at issue in this case), these alleged injuries are clearly insufficient to establish standing for declaratory and injunctive relief because they all occurred in the past. Plaintiffs discuss their categories of injury at length in their opposition, *see* NTEU Mem.

[1] Injunctive and declaratory relief is the only possible relief in this action raising a constitutional claim under the Fifth Amendment Due Process Clause: Money damages are not available because the United States has not waived sovereign immunity for these alleged harms, and an action under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971), which Plaintiffs do not bring, is 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).

8-16, but they never explain how these past injuries are sufficient for future injunctive relief under *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). Indeed, Plaintiffs cite *Lyons* only once in their opposition with a 'Cf.' notation. NTEU Mem. 18. Plaintiffs' alleged past injuries fail to establish standing for declaratory and future injunctive relief.

B. Plaintiffs' Alleged Future Injuries Fail To Establish Standing For Declaratory And Injunctive Relief.

Plaintiffs clarify in their opposition that they allege two forms of future injury—the only relevant injuries for a plaintiff seeking forward-looking injunctive relief. First, Plaintiffs contend that they face an increased risk of future harm, in the form of possible "identity theft," "harassment, intimidation, and coercion," and "emotional distress and anxiety." *Id.* at 18 (citing Am. Compl. ¶¶ 92-94). Second, Plaintiffs contend that they will be injured because their personal information remains in OPM's systems and is at "substantial risk of further unauthorized access." *Id.* at 16-17 (citing Am. Compl. ¶¶ 87-91). Both theories of future injury fail to establish standing for declaratory and injunctive relief.

Contrary to Plaintiffs' contention, NTEU Mem. 18, the increased risk of future harm in the form of possible identity theft or other speculative harms does not establish injury in fact under Article III. As an initial matter, Plaintiffs cannot claim that "the 'increased risk' [of future injury] is *itself* concrete, particularized, and *actual* injury for standing purposes," as this Circuit has expressly rejected that contention. *Pub. Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1297 (D.C. Cir. 2007). Instead:

> [T]he proper way to analyze an increased risk-of-harm claim is to consider the ultimate alleged harm – such as death, physical injury, or property damage . . . – as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently "imminent" for standing purposes.

Id. at 1298. To meet this test, Plaintiffs cannot merely assert that they are at an increased risk of future harm. NTEU Mem. 16-18. Indeed, the D.C. Circuit has recognized that there is a "powerful

argument that 'increased-risk-of-harm' claims . . . fail to meet the constitutional requirement that a plaintiff demonstrate harm that is 'actual or imminent, not conjectural or hypothetical.'" *Pub. Citizen Inc.*, 489 F.3d at 1294 (internal citation omitted)[2]; *see also Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) ("Allegations of possible future injury do not satisfy the requirements of Art. III."). The reason is simple: "Allowing a party to assert such remote and speculative claims [of possible future harm to its members] to obtain federal court jurisdiction threatens . . . to eviscerate the Supreme Court's standing doctrine." *Pub. Citizen Inc.*, 489 F.3d at 1294.

For these reasons, the vast majority of courts have rejected, as speculative, the claim that an increased risk of identity theft can justify standing. *See* OPM Mem. Supp. Mot. Dismiss Consol. Am. Compl. 26-30 (ECF No. 72-1); OPM Reply Mem. Supp. Mot. Dismiss Consol. Am. Compl. ("OPM Mem.") 4-5 (ECF No. 87). *See also In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litigation "SAIC*," 45 F. Supp. 3d 14, 26 (D.D.C. 2014) ("The degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending."); *see also Chambliss v. Carefirst, Inc.*, No. RDB-15-2288, 2016 WL 3055299, at *4 (D. Md. May 27, 2016), *appeal docketed*, No. 16-1737 (4th Cir. July 5, 2016); *Khan v. Children's Nat'l Health Sys.*, No. TDC-15-2125, 2016 WL 2946165, at *5-6 (D. Md. May 19, 2016); *In re SuperValu, Inc.*, No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016), *appeal docketed*, No. 16-2378 (8th Cir. May 26, 2016); *Fernandez v. Leidos*, *Inc.,* 127

[2] *Public Citizen* recognized that the D.C. Circuit "has not closed the door to all increased risk-of-harm cases," and has "allowed standing when there was at least *both* (i) a *substantially* increased risk of harm and (ii) a *substantial* probability of harm with that increase taken into account." 489 F.3d at 1295 (citation omitted). Even if this principle applies in this case – and the D.C. Circuit has suggested that it may not, *id.* ("[o]utside of increased exposure to environmental harms, hypothesized 'increased risk' has never been deemed sufficient 'injury'" (quoting *Ctr. for Law & Educ. v. Dep't of Educ.*, 396 F.3d 1152, 1160 (D.C. Cir. 2005))), it would not provide Plaintiffs relief. As *Public Citizen* recognized, "[i]n applying the 'substantial' standard, we are mindful, of course, that the constitutional requirement of imminence as articulated by the Supreme Court – even if this Court has said it does not completely bar increased-risk-of-harm claims – necessarily compels a very strict understanding of what increases in risk and overall risk levels can count as 'substantial.'" *Id.* at 1296. Plaintiffs make no attempt to satisfy this test.

F. Supp. 3d 1078, 1088 (E.D. Cal. 2015), *appeal docketed*, No. 15-17285 (9th Cir. Nov. 19, 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 366-67 (M.D. Pa. 2015). Here, Plaintiffs fail to show that they face a "certainly impending" threat of identity theft or other future harm. *See* NTEU Mem. 16-17; *see also Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1148 (2013) ("The party invoking federal jurisdiction bears the burden of establishing standing." (internal citation omitted)).

Plaintiffs fare no better by alleging that their personal information in OPM's systems is at risk of being accessed by an unauthorized individual in the future. NTEU Mem. 16-17. This theory is entirely speculative and fails for the same reasons as Plaintiffs' previous contention regarding future misuse. Plaintiffs fail to show that there is a certainly impending threat that their information will be accessed by an unauthorized individual in the imminent future. Plaintiffs' access theory also fails for an additional reason. The mere possibility of future unauthorized access is not sufficient to establish an Article III injury. Instead, for the loss of data to be a concrete and imminent injury, the information must, at a minimum, be disclosed to a third party. *See SAIC*, 45 F. Supp. 3d at 28 ("If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated."). Here, Plaintiffs offer nothing but speculation that their information faces the risk of "unauthorized access" by an unidentified third-party in the future, and such access is insufficient to establish a concrete and actual injury.

Plaintiffs also fail to establish, in their opposition, that they face a "substantial probability" that they will suffer future injuries that will be remedied by the specific injunctive relief they have sought. *See Afifi,* 101 F. Supp. 3d at 108 ("In this Circuit, a plaintiff must show a substantial probability of injury to establish imminent injury" (quoting *Sierra Club v. Jewell*, 764 F.3d 1, 7 (D.C. Cir. 2014))); *see also DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (explaining that standing is a claim- and relief- specific doctrine).

In their opposition, Plaintiffs fail to demonstrate the "substantial probability" of "imminent" future injury that this Circuit requires. Two of the three forms of injunctive relief they seek—an order requiring the revamping of OPM's data security policies and an order prohibiting OPM from collecting NTEU member's information—depend entirely on the claim that there will be another cyberattack on OPM's systems in the future that will necessarily compromise Plaintiffs' information. *See* NTEU Mem. 22-24 (discussing Am. Compl. 34-35, Request for Relief ¶¶ B-D). Such a claim stacks supposition on top of supposition: (1) that unknown entities intend to target OPM's systems; (2) that those entities have the capacity to target OPM's systems; (3) that those entities actually will target OPM in the imminent future; (4) that they will be successful in targeting OPM's systems in the imminent future; and (5) that a named Plaintiff's information will actually be compromised during this attack. *See also* OPM Mem. 6-10. Plaintiffs make no attempt to demonstrate this causal chain in their Amended Complaint or Opposition. Instead, Plaintiffs contend that their personal information, along with that of millions of others, continues to reside on OPM's systems and that OPM allegedly continues to have inadequate security measures, as evidenced by reports issued by OPM's Office of the Inspector General ("OIG") in November 2015 and May 2016 and by OPM's alleged inability to secure an able IT contractor. NTEU Mem. 17 (citing NTEU Am. Compl. ¶¶ 87-91). But even assuming for purposes of this motion certain inadequacies 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. *See Lyons*, 461 U.S. at 106; *Jewell*, 764 F.3d at 7.

Nor can Plaintiffs establish standing for their requested injunction requiring OPM to provide them lifetime credit monitoring services. This relief is based on the theory that Plaintiffs' information may be used by unknown thieves to commit financial fraud at an unknown point in the future. *See, e.g.*, NTEU Mem. 17-18. But, as discussed, this type of speculative future injury does

not suffice to establish standing for injunctive relief. In addition, Plaintiffs ignore the fact that Congress has already provided individuals affected by the OPM data breach with "complimentary identity protection coverage" that "is effective for a period of not less than 10 years," or until 2025. *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113 § 632, 129 Stat. 2242, 2470-71 (2015). Plaintiffs have not claimed that the identity theft protection they seek would be any different than the services to which they are already entitled, and any potential future injury occurring a decade from now can hardly be called "immediate." *See SAIC*, 45 F. Supp. 3d at 26; *Storm,* 90 F. Supp. 3d at 366-67 (discussing Article III's "strict imminency standard").

Plaintiffs' reliance on *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 693 (7th Cir. 2015), *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197, 1206-07 (N.D. Cal. 2014), and *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 954-55 (S.D. Cal. 2014), to support their claim for injunctive relief is misplaced. These cases do not address whether a claim for injunctive relief, the claims that Plaintiffs bring here, was sufficient to satisfy the requirements for prospective relief articulated in *Lyons*. And as OPM explained in its Motion to Dismiss the Consolidated Amended Complaint, these cases are in the clear minority and are factually distinguishable because they concern allegations of substantial and widespread misuse of stolen financial account information. *See* OPM Mem. Supp. Mot. Dismiss Consol. Am. Compl. 29. Moreover, the trend of district courts either declining to follow *Neiman Marcus* or factually distinguishing it has only continued since the filing of OPM's Motion. *Attias, v. CareFirst,* No. 15-cv-0882 (CRC), 2016 WL 4250232 (D.D.C. August 10, 2016); *Torres v. Wendy's Co.*, 2016 U.S. Dist. LEXIS 96947 (M.D. Fla. July 15, 2016); *Duqum v. Scottrade, Inc.*, No. 4:15-cv-1537-SPM, 2016 WL 3683001, *5-6 (E.D. Mo. July 12, 2016); *Bradix v. Advance Stores Co.*, No. 16-4902, 2016 WL 3617717 (E.D. La. July 6, 2016); *Chambliss,* 2016 WL 3055299; *Khan,* 2016 WL 2946165, at *3-4; *See also In re*

Zappos.com, Inc., 108 F. Supp. 3d 949, 955 (D. Nev. 2015) (listing post-*Clapper* cases where claims based on the future risk of identity theft/fraud were dismissed for lack of standing).

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

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

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

Plaintiffs discuss, at length, in their opposition the extent to which federal courts have recognized the existence of the constitutional right to informational privacy. *See* NTEU Mem. 25-31. But the Court need not determine, in this motion, whether the constitutional right to informational privacy exists. Instead, the much narrower issue here is whether the assumed constitutional right to informational privacy could impose a duty on the federal government to protect personal data—already subject to the Privacy Act's protections—from third-party theft. Under both Supreme Court and D.C. Circuit precedent, the answer is clearly 'no.'

Supreme Court precedent addressing the constitutional right to informational privacy does not support Plaintiffs' claim here. *See* OPM Mem. 15-22. Plaintiffs ignore in their opposition the critical limitations that the Supreme Court has established for any informational privacy right that may have constitutional roots. *See* NTEU Mem. 25-31. These limitations do not support Plaintiffs' theory that the Constitution imposes an obligation on the federal government to protect data from third-party theft. In summary:

(1) The Supreme Court has never held that the constitutional right to informational privacy requires the government to protect data from third-party theft; instead, the Court merely has assumed that the Constitution might provide certain limits on a state or federal government's ability to collect certain personal information through passage of a state or federal statute or an agency rule;

(2) The Court has specifically recognized that the Privacy Act's protections are sufficient to satisfy any constitutional privacy concerns even if an individual's information could be affected by a data breach at a federal agency; and

(3) The Court has emphasized that the government is entitled to considerable deference in exercising its responsibility as an employer, and in particular with respect to its information-security program, making any attempts to constitutionalize federal data security in this context inappropriate.

OPM Mem. 15-22. Plaintiffs neither address these critical issues in their opposition, nor offer any reasoned explanation for how their claim is grounded in Supreme Court precedent.

D.C. Circuit precedent likewise precludes Plaintiffs' constitutional claim. Plaintiffs do not dispute in their opposition that the handful of cases in the D.C. Circuit squarely addressing the assumed constitutional right to informational privacy addressed whether the government's collection of information, pursuant to a particular statute or rule, was consistent with the assumed informational privacy right. *See* OPM Mem. in Supp. of Mot. to Dismiss NTEU Pls.' Am. Comp. ("OPM Mem. in Supp.") 20 n.12 (ECF No. 81-1) (citing *Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786 (D.C. Cir. 1997); *United Steelworkers of Am., AFL-CIO-CLC v. Marshall*, 647 F.2d 1189 (D.C. Cir. 1980); *Franklin v. Dist. of Columbia*, 163 F.3d 625 (D.C. Cir. 1998); *Nat'l Fed'n of Fed. Emps. v. Greenberg*, 983 F.2d 286 (D.C. Cir. 1993)); NTEU Mem. 29-31. Nor have Plaintiffs cited any case from the D.C. Circuit (or any other Circuit for that matter) that supports their novel 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 theft and misuse by a third party.

Instead of grounding their constitutional theory in controlling precedent, Plaintiffs cite various cases from other circuits that are nonbinding and in any event irrelevant. *See* NTEU Mem. 32-37 (citing *Fadjo v. Coon*, 633 F.2d 1172 (5th Cir. 1981); *Eagle v. Morgan*, 88 F.3d 620 (8th Cir. 1996); *Sheets v. Salt Lake County*, 45 F.3d 1383 (10th Cir. 1995)). These cases provide no authority for the proposition that the Constitution imposes a duty on the federal government to protect data from

third-party theft. To the contrary, all of these cases, as Plaintiffs themselves recognize, *see* NTEU Mem. 36, involve situations where state officials deliberately and intentionally revealed private information to a particular person or to the public without adequate justification. But that situation is not present here. No Plaintiff is alleging that OPM deliberately decided to disclose a particular Plaintiff's personal information to another person or to the public at large for improper purposes. This case, instead, concerns a third-party cyberattack on OPM's information systems. Therefore, *Fadjo*, *Eagle*, and *Sheets* do not support Plaintiffs' claims here.

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

Plaintiffs do not dispute that the federal government's constitutional duty of care to protect against third-party harm can only be triggered here if the government "takes a person into its custody and holds him there against his will." *DeShaney v. Winnebago Cty. Dep't of Social Servs.*, 489 U.S. 189, 199-200 (1989); *see also* OPM Mem. in Supp. 22-25 (explaining basis for dismissal under *DeShaney*). Nonetheless, relying solely on a law review article, Plaintiffs argue that the federal government's custody and control of an individual's personal information should be considered a restraint of personal liberty triggering the protections of the Due Process Clause. NTEU Mem. 37 (citing A. Michael Froomkin, *Government Data Breaches*, 24 Berkley Tech. L. J. 1019, 1049 (2009)). Adopting the article's analysis, Plaintiffs contend that having their information on a government server is similar to being physically imprisoned because, like someone imprisoned against their will, they are "unable to exert any control whatsoever over how the government stores and secures" their data. NTEU Mem. 37 (citing Froomkin at 1049). This analogy is meritless. The governmental act of taking away someone's physical liberty is fundamentally different than keeping custody of information on a government server. When someone is incarcerated or institutionalized they are unable to provide for their most basic human needs—food, clothing, shelter, medical care, and reasonable safety—which is why the state has a corresponding constitutional duty to provide some

level of affirmative care. *Deshaney*, 489 U.S. at 200. Here, Plaintiffs obviously do not complain about their loss of liberty or their corresponding inability to provide for their basic human needs. They instead complain about their information being in OPM's systems and their relative inability to control how the data is stored and secured. But retaining custody of information and deciding the best way to secure it does not restrict anyone's physical liberty, and thus these decisions do not trigger any constitutional duty of care under the Due Process Clause. Plaintiffs' strained analogy that "custody" of data is akin to physical custody in a prison should be rejected. *See Colbert v. Dist. of Columbia*, 5 F. Supp. 3d 44, 58 (D.D.C. 2013) ("[T]his Court is bound to a narrow interpretation of 'custody' for the purpose of triggering a constitutional duty of care.").

Plaintiffs also argue, throughout their opposition, that OPM's alleged promise in Standard Form ("SF") 86 to handle investigative information in accordance with the requirements of the Privacy Act should have constitutional consequences: Plaintiffs argue that "[t]he constitutional right to informational privacy protects inherently personal information provided to the government on the promise of confidentiality, and it provides a basis for a claim where, as here, the government disregards that promise." NTEU Mem. 1; *see also id.* 2, 31, 32, 36, 37, 40, 41, 43, 44. But the SF-86's routine disclosure statement, regarding the Privacy Act, is not an enforceable promise under any contractual theory, let alone a promise that triggers an affirmative duty to protect under the Due Process Clause. As the Supreme Court explained in *Deshaney*, "the affirmative duty to protect arises not from the State's knowledge of the individual's predicament or from its expressions of intent to help him, but from the limitations which it has imposed on his freedom to act on his own behalf, through imprisonment, institutionalization, or other similar restraint of personal liberty." *DeShaney*, 489 U.S. at 190. Plaintiffs do not plead any state-imposed restraint on their liberty, and thus they fail to state a claim under the Due Process Clause.

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

To state a substantive due process claim based on executive conduct, a plaintiff must plead facts showing that the government engaged in conduct "so egregious, so outrageous, that it may fairly be said to shock the contemporary conscience." *Fraternal Order of Police Dep't of Corr. Labor Comm. v. Williams*, 375 F.3d 1141, 1144-45 (D.C. Cir. 2004) (quoting *Cty. of Sacramento v. Lewis*, 523 U.S. 833, 847 n.8 (1998)). Plaintiffs acknowledge in their opposition that, at a minimum, this standard requires them to plead facts showing that OPM acted in a deliberately indifferent manner. NTEU Mem. 43; *see also Estate of Phillips v. Dist. of Columbia*, 455 F.3d 397, 403 (D.C. Cir. 2006) ("If the plaintiff alleges that the government official failed to act . . . he must show that the official was at least deliberately indifferent to his constitutional rights."). This "stringent requirement exists to differentiate substantive due process, which is intended only to protect against arbitrary government action, from local tort law." *Butera v. Dist. of Columbia*, 235 F.3d 637, 651 (D.C. Cir. 2001) (citation omitted).

Plaintiffs argue that they have met this stringent requirement because, "OPM's conscious and continued failure to safeguard its databases . . . showed a reckless indifference to its obligation to protect the information's confidentiality." NTEU Mem. 43 (citation omitted). Plaintiffs rely heavily on the fact that the OPM Office of Inspector General ("IG") conducted required audits under the Federal Information Security Management Act, and concluded that OPM was not in compliance with certain information-security rules and standards. NTEU Mem. 41-43. But as the IG reports cited by Plaintiffs make clear, they do not contain mandatory directives, but instead contain discretionary recommendations that require the agency to weigh the costs, benefits, and technical feasibility of implementation. *See*, *e.g.*, OPM OIG, Final Audit Report: Federal Information Security Management Act Audit FY 2015 (Nov. 10, 2015) at 8, https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-

audit-report-4a-ci-00-15-011.pdf. The IG reports, therefore, reflect the collaborative process through which OPM continuously identifies potential weaknesses and conducts a risk assessment to determine what actions should be taken to strengthen its security protocols. This decisionmaking process—involving "large-scale personnel and program decisions" made by government officials—is not the type of government conduct that shocks the contemporary conscience. *Williams*, 375 F.3d at 1145 (citing *Lewis*, 523 U.S. at 849). Plaintiffs do not address this precedent in their opposition, or otherwise explain how a federal agency's programmatic decisions, like OPM's here, could rise to the level of conscience-shocking behavior.

Plaintiffs cite only one case—*Smith v. District of Columbia*, 413 F.3d 86 (D.C. Cir. 2005)—in support of their novel contention that a federal agency's information security program can be administered in a conscience-shocking manner. NTEU Mem. 43. But *Smith* is wholly inapplicable. There, a juvenile delinquent was murdered while in the custody of the District of Columbia at his government-provided apartment, and the evidence at trial showed, among other things, that the District had no standards whatsoever for selecting and monitoring the independent contractor responsible for overseeing the apartment complex, and the District had taken no noteworthy steps in response to multiple violent assaults at the youth's apartment. *Smith*, 413 F.3d at 92. This data breach case does not involve any facts that are even remotely similar to those in *Smith*. Regardless of whether OPM in hindsight could have or should have adopted a particular information security safeguard at a particular point in time, OPM's actions clearly do not amount to an "executive abuse of power . . . which shocks the conscience." *Williams*, 375 F.3d at 1145 (quoting *Lewis*, 523 U.S. at 846). Plaintiffs' constitutional claims, premised on the Due Process Clause, therefore should be dismissed.

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

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). But nowhere in their Amended Complaint or in their Opposition do Plaintiffs identify what statute 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).

Plaintiffs instead argue in their opposition that the Court's equitable powers allow for the relief they request. NTEU Mem. 44-45. In support, they cite two cases where injunctive relief was provided under 5 U.S.C. § 706(1) of the Administrative Procedure Act, *Cobell v. Norton*, 240 F.3d 1081 (D.C. Cir. 2001) and *Vietnam Veterans of America v. CIA,* 288 F.R.D. 192 (N.D. Cal. 2012), and one case where relief was granted under the remedial provisions of the Social Security Act, *New York v. Heckler*, 578 F. Supp. 1109 (E.D.N.Y. 1984). Those cases are inapposite, however, because in each of them, the plaintiffs identified a waiver of sovereign immunity separate from the court's equity powers. Plaintiffs here have provided no such waiver. Plaintiffs' request for lifetime credit monitoring services, accordingly, is barred by sovereign immunity.

CONCLUSION

For all the reasons stated above, and those articulated in OPM's opening memorandum, the *NTEU* action should be dismissed pursuant to Federal Rules of Civil Procedure 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/ *Andrew E. Carmichael*
MATTHEW A. JOSEPHSON
ANDREW E. CARMICHAEL
JOSEPH BORSON
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Room 7218
Washington, DC 20530
Tel: (202) 514-3346
Email: Matthew.A.Josephson@usdoj.gov
Email: Andrew.E.Carmichael@usdoj.gov

Dated: August 29, 2016

***Counsel for Federal Defendant* OPM**

CERTIFICATE OF SERVICE

I hereby certify that on August 29, 2016, I filed the above motion with the Court's CM/ECF system, which will send notice of such filing to all parties.

/s/ *Andrew E. Carmichael*
Andrew E. Carmichael