IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY LITIGATION This Document Relates To: *NTEU v. Cobert*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	Misc. Action No. 15-1394 MDL Docket No. 2664

NTEU Plaintiffs' Opposition to Defendant's
Motion to Dismiss Under Rule 12

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page:

Cases

Statutes

Other Authorities

Plaintiffs National Treasury Employees Union (NTEU), Eugene Gambardella, Stephen Howell, and Jonathon Ortino (collectively, NTEU Plaintiffs) respectfully submit this opposition to the Office of Personnel Management's (OPM) motion to dismiss their amended complaint (Mot.).

OPM's argument is that, no matter how lax its information technology security, it cannot be held accountable for the hackings of its information systems that were announced in June 2015. Through those hackings, unknown individuals repeatedly entered OPM's data systems and downloaded sensitive personal information that millions of individuals, including thousands of NTEU members, provided to OPM based on an explicit promise of confidentiality. There is no limiting principle to OPM's position. In its view, "leaving all the doors and windows open" to thieves seeking the sensitive personal information of federal public servants, despite nearly a decade of public admonitions from its own Inspector General, cannot implicate the constitutional right to informational privacy.[1]

The 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. OPM's argument that the right does not include a duty to protect that information is incompatible with the nature of the right and would render it hollow.

[1] See OPM: Data Breach: Hearing Before H. Comm. on Oversight and Gov't Reform, 114th Cong. (2015) ("According to the last eight years of IG reports, OPM's data security posture was akin to leaving all the doors and windows open at your house.") (statement of Chairman Jason Chaffetz).

NTEU Plaintiffs have sufficiently alleged that OPM violated NTEU members' constitutional right to informational privacy by disregarding its Inspector General's urgent security warnings for nearly a decade, leading to a series of data breaches that exposed inherently personal information that NTEU members provided to OPM on the promise of confidentiality. NTEU Plaintiffs have standing to bring their claim because they suffered a cognizable injury when their personal information was taken from OPM's databases. They have further established standing because one of the representative plaintiffs was subjected to a fraudulent tax return and unauthorized credit card charges believed to be caused by the data breaches. For these reasons, OPM's motion should be denied.

FACTUAL BACKGROUND

In June 2015, OPM made two separate announcements concerning data breaches that implicated the personal information of approximately 21.5 million individuals. On June 4, 2015, OPM announced it had uncovered a data breach involving hackers downloading from OPM's information systems the names, addresses, dates and places of birth, and Social Security Numbers of approximately 4.2 million employees, including thousands of NTEU members. Amended Complaint (Am. Compl.) ¶¶ 13, 15, 16. OPM first detected the data breach in April 2015, and it is believed to have been perpetrated in October 2014. Id. ¶ 14.

On June 12, 2015, OPM announced it had uncovered another data breach involving hackers downloading from OPM's information systems the background investigation materials of prospective, current, and former federal employees. Id. ¶¶ 18-19. Approximately 21.5 million individuals had their personal information

exposed through this breach, including thousands of NTEU members. Id. ¶¶ 19, 74. OPM first detected the breach in May 2015, and it is believed to have been perpetrated in July and August 2014. Id. ¶ 18. During this period, the perpetrators of the breach repeatedly accessed and took personal information from OPM's data systems related to background investigations that it has conducted. Id. ¶¶ 18-19.

The standard forms that federal employees must submit for their background investigations require them to disclose, or authorize OPM to obtain, among other information, Social Security numbers, past criminal history, disciplinary problems, academic background, marital information (including marital problems), past drug or alcohol use, police records, financial data, and medical information (including mental health issues). Id. ¶¶ 19-32. This information was among the information exposed in the breach announced on June 12, 2015. Id.

The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, et seq., tasks each agency head with safeguarding agency information systems and taking steps to reduce the risk of unauthorized use of information in the agency's possession. Am. Compl. ¶ 36. FISMA requires that agency heads comply with FISMA and the technology policies, procedures, standards, and guidelines established by appropriate authorities, e.g., executive orders on cybersecurity and standards issued by the National Institute of Standards and Technology (NIST). Id. ¶ 37.

In its FISMA audit for fiscal year 2014, OPM's Office of Inspector General (OIG) documented numerous deficiencies in OPM's information technology security

programs and practices. Id. ¶ 41. In congressional testimony, OPM Assistant Inspector General for Audits, Michael R. Esser, stated that some of these problems dated back to fiscal year 2007. Id. ¶ 43. Mr. Esser testified, for example, that OPM's security governance constituted a "material weakness" for fiscal years 2007 through 2013, and a "significant deficiency" in 2014. Id. ¶ 44. A "material weakness" is a "severe control deficiency that prohibits the organization from adequately protecting its data," and a "significant deficiency" means that the technical infrastructure remains "inherently difficult to protect." Id.

The Office of Management and Budget (OMB) requires all federal information systems to have a valid "authorization." Id. ¶ 45. An "authorization" is a "comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment." Id. Mr. Esser, however, testified that eleven OPM information systems were operating without a valid authorization. Id. Accordingly, Mr. Esser testified, "the volume and sensitivity of OPM's systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program." Id. ¶ 46. He recommended that the eleven systems operating without authorization be shut down in 2014, but OPM rejected his recommendation. Id. ¶ 45.

Mr. Esser further testified that the 2014 audit report revealed that "two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication of IT systems using

personal identity verification (PIV) credentials" to verify employees' identities. Id. ¶ 47. "Configuration management" relates to the "policies, procedures, and technical controls used to ensure that IT systems are securely deployed." Id. ¶ 48. As of 2014, some of OPM's regular system vulnerability scans "were not working correctly because the tools did not have the proper credentials," and some servers were not scanned at all. Id. And despite OMB requirements, "none of the agency's major applications" required PIV authentication, which, if implemented, would require that a hacker compromise more than a username and password to gain access to a system. Id. ¶ 50. Nor did OPM perform the basic cybersecurity practice of encrypting data. Id. ¶¶ 51-52.

Additionally, federal guidelines require agencies to develop and maintain an inventory of its information systems and audit all activities associated with those information system configurations. Id. ¶ 49. According to Mr. Esser, however, OPM did not maintain an accurate centralized inventory of all servers and databases. Id. "[W]ithout a comprehensive list of assets that need to be protected and monitored," Mr. Esser noted, even if all of its security features were being used appropriately, OPM could not "fully defend its network." Id.

As Mr. Esser summed up in June 2015, "some of the current problems and weaknesses were identified as far back as Fiscal Year 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today." Id. ¶ 54. OPM's Inspector

General, Patrick McFarland, agreed that OPM's cybersecurity shortcomings "without question . . . exacerbated the possibility" of a breach. Id. ¶ 56.

OPM continues to ignore the longstanding recommendations of its OIG, raising the substantial likelihood of another breach. Id. ¶¶ 87-91. In its fiscal year 2015 audit report released on November 10, 2015, OPM's OIG reiterated that, "for many years, we have reported critical weaknesses in OPM's ability to manage its IT environment, and warned that the agency was at an increased risk of a data breach." Id. ¶ 88 (adding that its "recommendations appeared to garner little attention, as the same findings were repeated year after year"). In light of "the overall lack of compliance that seems to permeate the agency's IT security program," the OIG concluded that it was "very concerned that the agency's systems will not be protected against another attack." Id.

Other signs of the substantial likelihood of another breach continue to mount. On May 9, 2016, the vendor that OPM hired to overhaul its information technology infrastructure "abruptly ceased operations," with another month left on its contract and the status of its work unknown. Id. ¶ 90 (noting vendor's "troubled history with government contracting"). On May 18, 2016, OPM's OIG issued an interim status report, stating that, having reviewed OPM's "recent Business Case" for its IT upgrades, it is "even more concerned" about OPM's plans to update its IT security because it failed to perform the mandatory planning steps for such a project that OMB requires and likewise failed to develop a "realistic budget." Id. ¶ 91.

Plaintiffs NTEU, Stephen Howell, and Jonathon Ortino filed a complaint against OPM in the Northern District of California on July 8, 2015, alleging a violation of NTEU members' constitutional right to informational privacy and seeking declaratory and injunctive relief. Id. ¶ 2. That complaint was transferred to this Court on October 9, 2015. An amended complaint maintaining the same cause of action was filed on June 3, 2016, adding Plaintiff Eugene Gambardella.

STANDARD OF REVIEW

To survive a Rule 12 motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). A claim is facially plausible when the pleaded factual content "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. In evaluating a Rule 12 motion, the Court "must treat the complaint's factual allegations as true, and must grant plaintiff 'the benefit of all inferences that can be derived from the facts alleged.'" Prisology v. Fed. Bureau of Prisons, 74 F. Supp. 3d 88, 92 (D.D.C. 2014).

ARGUMENT

I. NTEU Plaintiffs Have Article III Standing To Bring Suit.

To establish standing, a plaintiff must show (1) an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) a sufficient causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury will be redressed by a favorable decision. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014). "At the pleading stage, general factual allegations of injury resulting from the defendant's

conduct may suffice." Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992). As discussed below, the NTEU Plaintiffs were—and continue to be—injured by OPM's repeated and prolonged failure to safeguard employees' personal information which resulted in the taking of that information in the data breaches announced by OPM in June 2015. NTEU Plaintiffs, therefore, have standing to pursue their claim that their constitutional right to informational privacy has been violated.

A. OPM's Failure to Safeguard NTEU Plaintiffs' Data Has Caused Them Injury in Fact.

1. NTEU Plaintiffs' Injuries Occurred When The Personal Information That They Provided to OPM Was Taken.

NTEU Plaintiffs' standing should be viewed through the prism of their particular claim. As the Supreme Court has recognized, standing "often turns on the nature and source of the claim asserted." Warth v. Seldin, 422 U.S. 490, 500 (1975). NTEU Plaintiffs' injuries for standing purposes should thus be analyzed separately from the injury of the plaintiffs asserting Privacy Act and negligence claims, among others, in the Consolidated Amended Complaint. See id.[2]

NTEU Plaintiffs allege that their constitutional right to informational privacy was violated when their personal information was taken by unauthorized persons. Thus, in light of their claim, their injury occurred and their standing arose

[2] See also Doe v. Chao, 540 U.S. 614, 617-18, 624-25 (2004) (plaintiff who was "concerned and worried" about disclosure of his Social Security number, without further harm, had no cause of action under the Privacy Act, but might still have standing under Article III); Krottner v. Starbucks Corp., 406 Fed. Appx. 129, 130-31 (9th Cir. 2010) (ruling that plaintiffs who feared future harm after their personal information was stolen "pled an injury-in-fact for purposes of Article III standing" but did not "establish[] a cognizable injury for purposes of their negligence claim").

when their data was breached—when it was taken from OPM's information systems by the hackers—regardless of how that data might later be used.

Though OPM argues to the contrary (Mot. at 13-14), its argument conflicts with the Second Circuit's decision in ACLU v. Clapper, which is squarely on point and illustrates NTEU Plaintiffs' standing here. See 785 F.3d 787 (2d Cir. 2015). There, plaintiffs challenged the constitutionality of a federal program which allowed the National Security Agency to collect "metadata associated with telephone calls made by and to Americans." Id. at 792. The government argued that the plaintiffs lacked standing because, although it was clear that the plaintiffs' metadata had been collected, the plaintiffs could only speculate about whether the government would ever review that data. Id. at 800-01.

The court examined the standing question in light of the particular constitutional claim asserted by the plaintiffs. Id. at 801. Because the plaintiffs were arguing that the government's collection of such data violated the Fourth Amendment's proscription against unreasonable searches and seizures, the Second Circuit concluded that they were injured as soon as the data was seized or collected. Id. ("Whether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them."). The court likewise ruled that plaintiffs also had standing to assert a First Amendment violation. Id. at 802. Specifically, the injury occurred at the moment their metadata was collected and their interest in keeping their associations and contacts private was implicated. Id.

Similarly, here, NTEU Plaintiffs assert that their constitutional right to informational privacy was violated. There is no dispute that there have been data breaches through which Plaintiffs Gambardella, Howell, and Ortino had their personal information taken from OPM's databases, which were not adequately secured. Am. Compl. ¶¶ 6-8, 13-19, 59-66. Neither is there any dispute that their stolen personal information is no longer private. Id. Therefore, consistent with the standing principles articulated in ACLU v. Clapper, NTEU Plaintiffs' constitutional injury occurred at the moment their personal information was taken. Just as the plaintiffs in ACLU v. Clapper did not need to establish that their metadata had actually been reviewed, neither is it required for NTEU Plaintiffs to establish that their private information has been used in some particular way.

The Court in Klayman v. Obama followed the same standing analysis as ACLU v. Clapper. See 142 F. Supp. 3d 172 (D.D.C. 2015), vacated as moot, 2016 U.S. App. LEXIS 6190 (D.C. Cir. Apr. 4, 2016). There, the Court found that plaintiffs, who were customers of Verizon Business Network Services (VBNS) when the government collected VBNS call records, had standing to challenge that collection on Fourth Amendment grounds. Id. at 186-87. Plaintiffs did not have to show that their call records were actually accessed and reviewed by someone, or show any other concrete harm, because the alleged constitutional violation occurred at the moment the phone records were collected. Id. at 187.

ACLU v. Clapper and Klayman v. Obama are consistent with other precedent holding that a Fourth Amendment violation occurs at the time of the wrongful

search or seizure. See United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990) (holding Fourth Amendment violation "is 'fully accomplished' at the time of an unreasonable government intrusion"); United States v. Leon, 468 U.S. 897, 906 (1984) (same). The constitutional right to have one's personal information kept private and not wrongfully disclosed, asserted in this case, is analogous to the Fourth Amendment right to not have one's property wrongfully seized. This Fourth Amendment precedent further shows that the violation of NTEU Plaintiffs' constitutional right to informational privacy was "fully accomplished" (Verdugo-Urquidez, 494 U.S. at 264) when the data breaches occurred and their personal information was taken.

2. Alternatively, NTEU Plaintiffs' Specific Injuries Satisfy the Injury in Fact Requirement.

Even if NTEU Plaintiffs' standing argument is not, as it should be, evaluated in light of the specific constitutional claim asserted, their injuries are more than sufficient to establish injury in fact for standing purposes. Courts have found standing for data breach victims even where plaintiffs do not allege that actual identify theft or other harm has actually occurred. For example, in In re Adobe Systems, Inc. Privacy Litigation (In re Adobe), customers of a software company whose data was stolen claimed that the company had failed to maintain reasonable security measures which put them at increased risk of future harm. 66 F. Supp. 3d 1197, 1206-07 (N.D. Cal. 2014). In a commonsense analysis, the court concluded these plaintiffs had suffered a concrete and imminent threat of future harm sufficient to establish standing because the risk that the hackers might use the

stolen data was not speculative. See id. at 1216 ("why would hackers target and steal personal customer data if not to misuse it?"). Accord Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) (concluding that where the data breach is caused by a sophisticated thief, it is plausible to assume a substantial risk of harm: "Why else would hackers break into a store' database and steal consumers' private information?"). That same reasoning applies here, where sophisticated hackers breached OPM's systems repeatedly and took the information that they found. Am. Compl. ¶¶ 13-19.[3]

Similarly in In re Sony Gaming Networks and Customer Data Security Breach Litigation, plaintiffs alleged that Sony Gaming collected personal data, such as names, dates of birth, and credit and debit information, which was then hacked. 996 F. Supp. 2d 942, 954-55 (S.D. Cal. 2014). Most of the individual plaintiffs alleged they were at risk of future harm, but did not allege that they incurred any unauthorized charges stemming from the data breach. Id. at 956-58. The court held that the plaintiffs had standing. Id. at 962. It was not required that the plaintiffs allege that their personal information was accessed by some additional third party. Id. Instead, the plaintiffs "plausibly alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following the

[3] An intentional data breach by a knowledgeable hacker is thus distinguishable from cases such as In re Science Applications International Corp. Backup Tape Data Theft Litigation (In re SAIC), where data tapes were stolen by a "low-tech, garden-variety" car thief who might not have realized what the tapes were or how to access the information they contained. See 45 F. Supp. 3d 14, 25, 33 (D.D.C. 2014). OPM's reliance on this decision (Mot. at 9, 13) is, therefore, misplaced.

intrusion." Id. Accord Moyer v. Michaels' Store, Inc., 2014 U.S. Dist. LEXIS 96588, at *19 (N.D. Ill. July 14, 2014) (elevated risk of identity theft satisfies the injury-in-fact requirement even if plaintiff has not suffered a direct financial loss).

The Court in AFGE v. Hawley reached a similar conclusion in the Privacy Act context. See 543 F. Supp. 2d 44, 45 (D.D.C. 2008). The plaintiffs in that case brought a Privacy Act suit based on a federal agency's failure to safeguard sensitive personnel data. Id. at 45. Their claimed injury was based on the release of the data itself—distress and concern about future identify theft—and the Court concluded the employees had standing without regard to whether any third party had used their data because their "alleged injury is not speculative nor dependent on any future event, such as a third party's misuse of the data." Id. at 50-51.

Though OPM argues otherwise (see Mot. at 10 n.8, incorporating arguments by reference), the Supreme Court's decision in Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013), is not to the contrary. The plaintiffs there sought a declaration that a statute authorizing the surveillance of certain persons was unconstitutional under, inter alia, the First and Fourth Amendments. Id. at 1146. But the plaintiffs lacked standing, because they could not show that any surveillance—the initial act causing their alleged injury—had occurred, and could only claim that there was an "objectively reasonable likelihood" that such surveillance would occur in the future. Id. at 1147-50. And as the Court emphasized, the plaintiffs' claims rested on a highly speculative chain of events, such as the government deciding to target communications of foreign persons with

whom plaintiffs interacted, the judges on the Foreign Intelligence Surveillance Court approving the surveillance, and the government actually intercepting the communications between plaintiffs and their contacts. Id. at 1148. Compare id., with ACLU v. Clapper, 785 F.3d at 800-01 (distinguishing Clapper v. Amnesty Int'l and finding standing because the metadata of the plaintiffs had already been gathered, and so no speculative chain of events was at issue); Remijas, 794 F.3d at 694 ("[I]t is important not to overread Clapper [which] was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs."). Here, in contrast, there is no dispute that an actual theft of NTEU Plaintiffs' personal information has occurred.[4]

The Court in Clapper neither overruled the standing standard of other cases, nor established some new Article III framework. The Supreme Court has found possible future injury sufficient to establish standing in a variety of contexts, such as where someone's concern about being arrested was not "chimerical" or where fear of persecution was not "imaginary or wholly speculative" or where fears of arrest were "well-founded." Driehaus, 134 S. Ct. at 2337. Accord Remijas, 794 F.3d at 693 (Clapper should not be read to foreclose any use of future injuries to support Article III standing); In re Sony Gaming, 996 F. Supp. 2d at 961 (Clapper "did not set forth a new Article III framework" or "overrule previous precedent").

[4] Clapper, moreover, was decided on summary judgment (133 S. Ct. at 1146), which requires a greater degree of evidentiary proof than the motion to dismiss stage.

Thus, pre-Clapper Seventh and Ninth Circuit decisions holding that data breach victims have standing even if they do not allege any financial harm or concrete injury remain instructive. See Krottner v. Starbucks, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (plaintiffs whose personal information was stolen had standing to sue their employer over the theft because "anxiety and stress" and an increased risk of identity theft were sufficient injury in fact); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 633-34 (7th Cir. 2007) (bank customers whose personal information had been hacked, but not yet misused, had standing because the increased risk of future harm from possible misuse was sufficient injury in fact). Under those decisions and post-Clapper decisions like In re Adobe and In re Sony Gaming, an increased risk of future identity theft is sufficient to establish standing.

NTEU Plaintiffs, moreover, have alleged other types of injury. Plaintiff Eugene Gambardella had a false tax return filed in his name following the OPM data breaches that he reasonably attributes to the data breaches. Am. Compl. ¶¶ 79-83 (alleging that fraudulent tax return filed after OPM data breaches occurred; that Mr. Gambardella's personal information has not been exposed in any other data breach; and that Mr. Gambardella has not otherwise been the victim of identity theft). Mr. Gambardella further suffered financial harm when his tax refund of approximately $7000 was delayed because of this fraudulent return. Id. ¶ 81. He also incurred fraudulent credit card charges that he believes stem from the OPM data breaches. Id. ¶¶ 82 (providing basis for belief that harm caused by OPM data breaches), 84. Courts have found that individuals whose stolen data has been

used have Article III standing, including situations in which the stolen data is alleged to have been used to incur fraudulent credit card charges or to file a fraudulent tax return. See, e.g., Remijas, 794 F.3d at 693-94, 697 (finding standing where data breach victims incurred fraudulent credit card charges and noting that "[a]lthough some credit card companies offer some customers 'zero liability' policies, under which the customer is not held responsible for any fraudulent charges, that practice defeats neither injury-in-fact nor redressability"); In re SAIC, 45 F. Supp. 3d at 29 (ruling that plaintiffs who alleged their data had been viewed and misused by a third party had been injured); Smith v. Triad of Alabama, LLC, 2015 U.S. Dist. LEXIS 132514, at *16-17, *24 (M.D. Ala. Sept. 2, 2015) (ruling that theft of Social Security Number and filing of fraudulent tax return with allegation of economic loss was sufficient injury); Longenecker-Wells v. Benecard Servs., Inc., 2015 U.S. Dist. LEXIS 126837, at *10 (M.D. Pa. Sept. 22, 2015) (concluding that filing of fraudulent tax returns, mitigation costs, and likelihood of future financial harm sufficient for standing). Thus, OPM's arguments that fraudulent credit card charges suffered by Mr. Gambardella are insufficient injury (Mot. at 12) are unfounded.[5]

3. NTEU Plaintiffs Sufficiently Allege Future Harm.

OPM argues that because injuries such as Mr. Gambardella's false tax return occurred in the past, NTEU Plaintiffs cannot seek forward-looking declaratory or injunctive relief. Mot. at 6-10. OPM is wrong because NTEU Plaintiffs do not

[5] OPM does not argue that Plaintiff Gambardella's fraudulent tax return is not a cognizable harm; it only argues that he cannot satisfy the traceability prong of standing (see Mot. at 10-11). As explained below, that argument is unfounded.

allege only past harm; they specifically allege that their personal information is at "substantial risk" of "further unauthorized access" and ground that allegation in recent reports by OPM's OIG and recent events. Am. Compl. ¶¶ 87-91.

In its fiscal year 2015 audit report, OPM's OIG reiterated that "the overall lack of compliance that seems to permeate the agency's IT security program" continues, and that it is "very concerned that the agency's systems will not be protected against another attack." Id. ¶ 88. On May 18, 2016, OPM's OIG issued an interim status report, reporting that, having reviewed OPM's "recent Business Case" for its IT upgrades, it is "even more concerned" about OPM's plans to update its IT security because it failed to perform the mandatory planning steps for such a project that OMB requires and likewise failed to develop a "realistic budget" for the effort. Id. ¶ 91. Indeed, OPM's inability to hire and retain an appropriate contractor to upgrade its information technology lend credence to the skepticism evinced by OPM's OIG. Id. ¶ 90. OPM hired a vendor with a "troubled history with government contracting" to overhaul its information technology infrastructure; on May 9, 2016, the vendor "abruptly ceased operations," with one month left on its contract and the status of its work unknown. Id.[6]

Thus, contrary to OPM's contention (Mot. at 6-10), NTEU Plaintiffs sufficiently allege a "substantial risk" of future unauthorized access of their

[6] OPM's argument—based entirely on a "Fact Sheet" that it authored—that it has "reduce[d] the possibility that another cyberattack may occur and negate[d] the need for judicial intervention" through IT improvements (Mot. at 10 n.7) is self-serving and, as indicated above, rebutted by the finding of its own, independent Inspector General.

inherently personal information, and they further allege that any future unauthorized access would further violate their constitutional right to informational privacy. Am. Compl. ¶¶ 87-91. Because NTEU Plaintiffs are "realistically threatened by a repetition" of the violation of their constitutional rights (Afifi v. Lynch, 101 F. Supp. 3d 90, 109 (D.D.C. 2015)), they have standing to seek declaratory and injunctive relief. See In re Adobe, 66 F. Supp. 3d at 1220, 1223 (ruling plaintiffs had standing to seek declaratory and injunctive relief stemming from data breach). Cf. City of Los Angeles v. Lyons, 461 U.S. 95, 109 (1983) (denying injunctive relief for single incident of violence unlikely to reoccur).

NTEU Plaintiffs also allege a substantial likelihood of "identity theft"; "harassment, intimidation and coercion"; and "emotional distress and anxiety." Am. Compl. ¶¶ 92-94. Contrary to OPM's assertion (Mot. at 13), these allegations are likewise sufficient to demonstrate injury in fact. See, e.g., Krottner, 628 F.3d at 1142 (emotional distress caused by theft of laptop containing personal information is sufficient Article III injury); Pisciotta, 499 F.3d at 632 (emotional distress resulting from data breach is sufficient Article III injury). Cf. Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) (emotional distress is insufficient for Article III injury where, unlike here, "no identifiable taking" of personal information occurred).

B. NTEU Plaintiffs' Injuries Are Fairly Traceable To OPM's Failure to Safeguard Their Personal Data.

To establish standing, a plaintiff must also show that the alleged injury is "fairly traceable to the challenged action of the defendant." Bennett v. Spear, 520 U.S. 154, 167 (1997). Accord Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d

963, 969 (7th Cir. 2016) ("Merely identifying potential alternative causes does not defeat standing."). Causation may be found even when, as here, there are multiple links in the chain connecting the defendant's conduct and the plaintiff's injury. Bennett, 520 U.S. at 168-69. There is, moreover, no requirement that the defendant's conduct be the last link in that chain. Id.

Causation is established if the government action complained about was "at least a substantial factor motivating the third parties' actions." Tozzi v. HHS, 271 F.3d 301, 308 (D.C. Cir. 2001). Accord Consumer Fed'n of Am. v. FCC, 348 F.3d 1009, 1012 (D.C. Cir. 2003) (causation is established "[w]hen an agency action permits a third party to engage in conduct that allegedly injures a person"). As pertinent here, courts have found that victims of data theft have standing to sue the entity supposedly safeguarding their data even where a third party, such as a hacker, was involved. See, e.g., In re Adobe, 66 F. Supp. 3d at 1220 (data breach victims' alleged injury was fairly traceable to software company's "failure to abide by its contractual obligation to provide 'reasonable . . . security controls'").

NTEU Plaintiffs' injuries from the OPM data breaches are fairly traceable to OPM's failure to safeguard their personal information. While a third party—the hacker—was the actual thief, OPM facilitated the hacking by ignoring its Inspector General and leaving its data systems vulnerable to attack. OPM had been amply warned about the failings in its data security measures. Am. Compl. ¶¶ 38-46, 49-52. It disregarded those warnings and violated information security safeguards set forth in statutes, regulations, and other federal mandates. See id. OPM, moreover,

has acknowledged publicly that the personal data of millions of employees has been exposed through its breaches, and it has contacted affected individuals, including Plaintiffs Gambardella, Howell, and Ortino, to let them know that they are at risk. Id. ¶¶ 13, 16, 18-19, 71-72. See Jewel v. NSA, 673 F.3d 902, 912 (9th Cir. 2011) (plaintiffs' injuries from widespread warrantless eavesdropping, namely invasion of privacy and violation of statutory protections, were traceable to government's surveillance program); ACLU v. Clapper, 785 F.3d at 801 (plaintiffs' injury from government collection of metadata is traceable to program allowing such collection).

Accordingly, once this Court accepts NTEU Plaintiffs' argument that all NTEU members implicated in the OPM data breaches were "injured" at the moment their data was taken from OPM's databases (see Section I.A.1 supra), the "fairly traceable" criterion is plainly met. See, e.g., Consumer Fed'n of Am., 348 F.3d at 1012; Tozzi, 271 F.3d at 308; In re Adobe, 66 F. Supp. 3d at 1220. Indeed, OPM does not contest this proposition. See Mot. at 13-14 (arguing no injury was suffered when data was taken, but omitting any argument that, if the Court finds to the contrary, traceability is not satisfied).

And contrary to OPM's contention (Mot. at 10-13), the "fairly traceable" criterion is likewise met if the Court accepts NTEU Plaintiffs' additional argument that Plaintiff Gambardella (and thus Plaintiff NTEU) suffered injury in fact when a fraudulent federal tax return was filed on his behalf, delaying, substantially, his receipt of the federal tax refund due to him and suffered further injury when he was the victim of unauthorized credit card charges. In In re SAIC, for example, a

plaintiff had standing to sue an information technology company over a data breach after a fraudulent loan application had been taken out in his name. See 45 F. Supp. 3d at 32. The fraudulent loan application was initiated by a third party but the court held that there was still sufficient causation between the injury caused by that fake loan application and the mishandling of plaintiff's sensitive personal information by the information technology company. Id. Similarly, in that same case, a plaintiff who received phone solicitations pitching medical products for a condition listed in the stolen medical records had standing to sue the information technology company even though a third party made the actual calls. Id. at 33.

Moreover, in Remijas, the Seventh Circuit rejected the defendant's argument that the plaintiffs could not prove traceability because their data might have been stolen through other data breaches. See 794 F.3d at 696. The Court concluded that such an argument "has no bearing on standing to sue; at most, it is a legal theory that [defendant] might later raise as a defense." Id. For causation purposes, "[i]t is enough at this stage of the litigation that [defendant] admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk." Id.

OPM argues that a fraudulent tax return cannot be "fairly traceable" to the OPM data breaches, relying on In re Horizon Healthcare Services, Inc. Data Breach Litigation, 2015 U.S. Dist. Lexis 41839 (D.N.J. March 31, 2015). Mot. at 10-11 (incorporating arguments by reference). But that case has no applicability here. The plaintiff in that case argued that a fraudulent tax return in his and his wife's

name had been filed, but his wife's personal information had not been among the stolen data. The plaintiff had to allege, therefore, that the thief might have used his personal information and "cobbled together" personal information for the wife "from other sources." Id. at *20 (emphasis added). The court found such a "remote possibility" insufficient for standing. Id. at *23. But there is no alleged cobbling together of information here. Am. Compl. ¶ 79 (fraudulent return filed on behalf of Plaintiff Gambardella only and did not purport to be a joint return). The personal identifying information necessary to file the fraudulent tax return—the name, address, and Social Security Number of Plaintiff Gambardella—was among the data stolen in the OPM data breaches. Id. ¶¶ 59-66.

C. Plaintiffs' Requested Relief Would Remedy Their Injuries.

NTEU Plaintiffs have also shown redressability. That is, they have shown that they "personally would benefit in a tangible way from the court's intervention." Steel Co. v. Citizens for Better Env't, 523 U.S. 83, 103 n.5 (1998). Indeed, this Circuit has liberally construed the redressability prong, holding that "'a party seeking judicial relief need not show to a certainty that a favorable decision will redress [its] injury.'" Teton Historic Aviation Found. v. Dep't of Def., 785 F.3d 719, 725-26 & n.5 (D.C. Cir. 2015) (concluding plaintiff met redressability and other standing criteria even though "[i]t is not altogether clear what exactly [plaintiff] believes it would receive from success in this action").

NTEU Plaintiffs request several forms of relief, each of which would remedy their injuries. First, NTEU Plaintiffs ask this Court to declare that OPM's failure to protect NTEU members' personal information was unconstitutional. Am. Compl.,

Request for Relief A. Declaratory and injunctive relief redress an injury where, as here, the harm to plaintiffs is continual and ongoing. NTEU members, including the individual NTEU Plaintiffs, continue to face a "substantial risk of further unauthorized access" of their personal information. Id. ¶¶ 87-91. And they likewise face a "substantial risk of identity theft" (or in the case of Mr. Gambardella, additional instances of identity theft). Id. ¶¶ 92. The requested relief is thus appropriate. See Ollier v. Sweetwater Union High Sch. Dist., 768 F.3d 843, 865 n.13 (9th Cir. 2014) ("Sweetwater's argument against redressability is premised on the idea that prospective injunctive relief cannot redress past harm. Because Plaintiffs' harm is ongoing, that argument fails."); ACLU v. Clapper, 785 F.3d at 801 (plaintiffs' injury from the government's collection of metadata would be redressed by a ruling striking down such program). In the data breach context, the court in In re Adobe held that the data breach victims' injury from an unauthorized data breach would be redressed by the requested declaratory judgment that the defendant failed its obligation to provide reasonable security measures and that the defendant must implement specified future security measures. See 66 F. Supp. 3d at 1220. That court's conclusions are equally applicable here.

Second, NTEU Plaintiffs seek an order that OPM provide lifetime credit monitoring and identify theft protection to affected NTEU members. Am. Compl., Request for Relief, B. This practical relief would remedy the loss of a sense of security that they have suffered. Id. ¶¶ 71-72, 94. See generally Remijas, 794 F.3d at 696-97 (data breach victims who had already been reimbursed for fraudulent

charges satisfied redressability prong because they might have mitigation expenses or other injuries in the future which would be remedied by a favorable ruling).

Third, NTEU Plaintiffs request an order that OPM take all necessary and appropriate steps to correct deficiencies in its IT security program. Am. Compl., Request for Relief, C. This relief would minimize the possibility of future breaches that would affect plaintiffs. See In re Adobe, 66 F. Supp. 3d at 1220 (data breach victims' request for a declaration that the defendant must implement specified future security measures satisfied Article III).

Lastly, NTEU Plaintiffs request that the Court enjoin OPM from collecting NTEU members' future personal information in electronic form until the Court is satisfied that all necessary and appropriate steps to safeguard such personal information have been taken. Am. Compl., Request for Relief, D. This relief would keep additional personal information from being exposed by any future breaches, for which NTEU Plaintiffs are at substantial risk (id. ¶¶ 87-91). See Klayman, 2015 U.S. Dist. LEXIS 151826, at *36-40 (plaintiffs alleging that collection of their phone records violated their constitutional rights had standing to seek order enjoining future collection of such data). Accord Jewel, 673 F.3d at 912.

D. Plaintiff NTEU Has Associational Standing to Bring Suit.

In light of the harm suffered by the individual plaintiffs discussed above, Plaintiff NTEU has associational standing here. "[A]n association has standing to bring suit on behalf of its members when (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane

to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." Hunt v. Wash. State Apple Adver. Comm'n, 432 U.S. 333, 343 (1977).

OPM's argues that NTEU does not have standing because no individual plaintiffs have standing. Mot. at 14. But, as explained above, each of the individual NTEU Plaintiffs has standing. See Consumer Fed'n of Am., 348 F.3d at 1011-12 (first prong of associational standing test satisfied if one member has standing). OPM does not argue that NTEU has failed to satisfy the other parts of the associational standing test. Nor could it. As the exclusive bargaining representative of approximately 150,000 federal employees in 31 federal agencies, NTEU frequently "enforc[es] employees' collective and individual rights in federal courts." Am. Compl. ¶ 5. Thus, the interests it seeks to protect here are germane to its purpose. See ACLU v. Clapper, 785 F.3d at 802 ("[A] union's 'standing to assert the First and Fourteenth Amendment rights of association and privacy of its individual members is beyond dispute.'"). NTEU, moreover, is not seeking relief that might require individualized proof. See Am. Compl., Request for Relief.

II. NTEU Plaintiffs Have Sufficiently Alleged A Breach Of The Constitutional Right To Informational Privacy.

NTEU Plaintiffs have sufficiently alleged a claim based on the constitutional right to informational privacy. As the Supreme Court has explained, the constitutionally protected "zone of privacy" involves "at least two different kinds of interests." See Whalen v. Roe, 429 U.S. 589, 598-600 (1977). The pertinent interest here is "the individual interest in avoiding disclosure of personal matters." See id.

at 599. This right, which is often referred to in case law and scholarship as the constitutional right to informational privacy, has been recognized by the Supreme Court, a strong majority of federal appellate courts, and judges of this Court for nearly four decades.

The right has a firmer grounding in federal jurisprudence and is more expansive than OPM suggests (see Mot. at 15-22). As discussed below, the right has two functions, one of which OPM ignores. In the first instance, it protects individuals from having to disclose inherently personal information to the government, absent a sufficient governmental interest in the information. But if such information is disclosed to the government, with a legitimate expectation of confidentiality, the right can serve as the basis for a claim if the government allows unauthorized access to that information. NTEU Plaintiffs have sufficiently alleged that the latter occurred here, violating their rights under the Constitution, including the Fifth Amendment Due Process Clause (Am. Compl. ¶¶ 95-98).

A. The Constitutional Right to Informational Privacy is Firmly Recognized.

The Supreme Court first recognized the constitutional right to informational privacy nearly forty years ago. In Whalen, the Supreme Court referred to the constitutional privacy "interest in avoiding disclosure of personal matters" while evaluating a state's practice of collecting names and addresses of all persons prescribed drugs with both legitimate and illegitimate uses. See 429 U.S. at 599-600. The patients who brought the suit argued that the state statute requiring the practice threatened to impair their nondisclosure interests, among others. Id. at

600. The Court analyzed the patients' claim, discussed their nondisclosure interests, and concluded that the state's patient-identification requirements did not "constitute an invasion of any right or liberty protected by the Fourteenth Amendment." Id. at 600-04. Accord id. at 606 (Brennan, J., concurring) ("The Court recognizes that an individual's 'interest in avoiding disclosure of personal matters' is an aspect of the right to privacy, but holds that in this case, any such interest has not been seriously enough invaded by the State to require a showing that its program was indispensable to the State's effort to control drug abuse.") (internal citation omitted).

The Supreme Court's unanimous decision in Whalen reflected an acknowledgement that, while "[t]he concept of a constitutional right of privacy still remains largely undefined," it includes, among other things, "the right of an individual not to have his private affairs made public by the government." See 429 U.S. at 599-600 & n. 24. See also Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S. Ct. Rev. 173, 212 (1979) (noting Whalen, among other Supreme Court decisions, reflects a view that "the Constitution creates a general right of privacy uncabined by any specific language in the Constitution"). In the same term that Whalen issued, the Supreme Court again acknowledged the constitutional right to informational privacy. See Nixon v. Admin. of Gen. Servs., 433 U.S. 425, 457-58 (1977) (discussing the constitutional privacy interest described in Whalen while evaluating statute requiring President to submit papers and tape recordings for archival review and screening).

In 2011, the Supreme Court had occasion to revisit the right. See NASA v. Nelson, 562 U.S. 134 (2011) (analyzing whether parts of standard background investigation form violated constitutional right to informational privacy). While the Court chose to assume, without deciding, that the right existed (see id. at 138), its decisions in Whalen, Nixon, and Nelson show that, since 1977, the Supreme Court has, on three occasions, analyzed claims based on the constitutional right to informational privacy. See Nelson, 562 U.S. at 159 ("[W]e conclude that the Government's inquiries do not violate a constitutional right to informational privacy.") (citing Whalen, 429 U.S. at 605); Nixon, 433 U.S. at 458-59 (analyzing whether forthcoming regulations would violate right); Whalen, 429 U.S. at 605 (analyzing whether state statute would violate right). As Nelson pointed out, moreover, two other Supreme Court opinions "have mentioned the concept in passing and in other contexts." See Nelson, 562 U.S. at 146 (citing Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762-63 (1989) and New York v. Ferber, 458 U.S. 747, 759 n.10 (1982)).

Nearly every federal court of appeals has taken the Supreme Court's cue and recognized the right. After Whalen and Nixon issued, the Second, Third, Fourth, Fifth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits recognized the constitutional right to privacy in the nondisclosure of personal information. See, e.g., Ferm v. United States, 194 F.3d 954, 958-60 (9th Cir. 1999) ("While the Supreme Court has expressed uncertainty regarding the precise bounds of the

constitutional 'zone of privacy,' its existence is firmly established.").[7] Only the Sixth Circuit has taken a different approach to the right. In J.P. v. DeSanti, it did not disavow the right's existence, but it concluded that "not all rights of privacy or interests in nondisclosure of private information are of constitutional dimension, so as to require balancing government action against individual privacy." See 653 F.2d 1080, 1089-91 (6th Cir. 1981).

The D.C. Circuit has not had occasion to rule squarely on the right's existence, and it has, in dicta, both acknowledged and questioned the right's existence. Several panels of the court have indicated a view that the right exists. See, e.g., United States v. Hubbard, 650 F.2d 293, 304-05 & nn.38-39 (D.C. Cir. 1980) (citing Whalen with approval and concluding that the Fifth Amendment's

[7] Accord Denius v. Dunlap, 209 F.3d 944, 955-56 (7th Cir. 2000) (recognizing constitutional right to privacy and evaluating information requested in disclosure form); Eagle v. Morgan, 88 F.3d 620, 625 (8th Cir. 1996) (recognizing constitutional right to privacy, but ruling that disclosure of individual's prior guilty plea did not violate right); Sheets v. Salt Lake Cnty., 45 F.3d 1383, 1388 (10th Cir. 1995) (recognizing constitutional right to privacy and ruling that deceased wife's diaries are protected by the right); James v. Douglas, 941 F.2d 1539, 1544 (11th Cir. 1991) (ruling complaint sufficiently alleged violation of constitutional right to privacy where it alleged police allowed unauthorized viewing of sex tape of plaintiff and spouse seized as evidence); Woodland v. City of Houston, 940 F.2d 134, 138 (5th Cir. 1991) (recognizing constitutional right to privacy and remanding to district court to weigh private and governmental interests implicated in pre-employment polygraph test); Walls v. Petersburg, 895 F.2d 188, 192-95 (4th Cir. 1990) (recognizing constitutional right to privacy and finding that required disclosures did not violate right); Barry v. City of New York, 712 F.2d 1554, 1558-64 (2d Cir. 1983) (recognizing constitutional right to privacy but upholding public financial disclosure requirement for certain city employees); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577-80 (3d Cir. 1980) (recognizing constitutional right to privacy but allowing government to examine employee medical records kept by employer).

"protection of liberty from federal intrusion . . . can be no less comprehensive" than the Fourteenth Amendment's "sphere of personal liberty"); Doe v. Webster, 606 F.2d 1226, 1238 n.49 (D.C. Cir. 1979) ("The right to privacy . . . 'should encompass a substantial measure of freedom for the individual to choose the extent to which the government could divulge criminal information about him, at least where no conviction has ensued and no countervailing government interest is demonstrated.'") (quoting Utz v. Cullinane, 520 F.2d 467, 482 n.41 (D.C. Cir. 1975)). Accord Nat'l Fed'n of Fed. Emps. v. Greenberg, 983 F.2d 286, 295-96 (D.C. Cir. 1993) (Edwards, J., concurring) ("I find no 'ambiguity' in the core principle undergirding the Supreme Court's decision in Whalen v. Roe . . . ."). Another panel of the court, in dicta, expressed doubts as to its existence. See AFGE v. HUD, 118 F.3d 786, 791-92 (D.C. Cir. 1997) (discussing precedent "suggest[ing] in dicta the existence of a constitutional right to privacy in personal information," but expressing "doubts" as to its existence). And two members of another panel, short of expressing such doubt, indicated they view Whalen to be ambiguous. Greenberg, 983 F.2d at 293-94 (rejecting request for preliminary injunction based on facial challenge to "voluntary" questionnaire).

In the absence of Circuit precedent to the contrary, four judges of this Court have embraced the clear majority view and have issued rulings based on the constitutional right. See Johnson v. Quander, 370 F. Supp. 2d 79, 102 (D.D.C. 2005) (Walton, J.) ("'The privacy interest asserted in this case falls within the first category referred to in Whalen v. Roe, the right not to have an individual's private

affairs made public by the government.'") (quoting Westinghouse, 638 F.2d at 577), aff'd, 440 F.3d 489, 502 (D.C. Cir. 2006); United States v. District of Columbia, 44 F. Supp. 2d 53, 60-62 (D.D.C. 1999) (Urbina, J.) (recognizing right and analyzing claim); NTEU v. Dep't of Treasury, 838 F. Supp. 631, 634-38 (D.D.C. 1993) (Greene, J.) (granting preliminary injunction where NTEU "challenge[d] certain questions on Standard Form SF-85P, Customs Form CF 257, and Treasury Department Form TD F 67-32.5 as invasive of their constitutional right to privacy"); Doe v. Di Genova, 642 F. Supp. 624, 634 (D.D.C. 1986) (Gasch, J.) (recognizing right and analyzing claim); see also Best v. District of Columbia, 1991 U.S. Dist. LEXIS 5435, at *5-7 (D.D.C. Apr. 23, 1991) (Oberdorfer, J.) (discussing Whalen and Nixon and acknowledging constitutional right in analysis of qualified immunity claim).[8]

In sum, the Supreme Court has spoken, and, in the almost forty years since then, nearly all of the courts of appeals and several judges of this Court have recognized the constitutional right to informational privacy.

B. The Right Requires the Government to Protect Personal Information Entrusted to it.

Once recognizing that the constitutional right to informational privacy protects inherently personal information from disclosure to the government, courts have concluded that, when individuals choose to provide such information to the government based on a promise of confidentiality, the government cannot disregard

[8] Judges of this Court have not uniformly embraced the constitutional right. See, e.g., Hensley v. Office of the Architect of the Capitol, 806 F. Supp. 2d 86, 91-92 (D.D.C. 2011) (Leon, J.); Goings v. Court Servs. & Offender Supervision Agency, 786 F. Supp. 2d 48, 74-75 (D.D.C. 2011) (Howell, J.).

that promise. In other words, the promise on which the government is permitted to obtain constitutionally protected personal information cannot be a hollow one. Thus, the right may serve as the basis for a claim where the government fails to adequately secure the information that it promised to safeguard.

OPM's motion omits mention of this core function of the right and incorrectly asserts that the government has no duty to protect personal data entrusted to it (Mot. at 15-22). But the cases discussed below show that a claim based on the constitutional right to informational privacy can be brought in a circumstance like this, where inherently private information was given to the government on the promise of confidentiality and that promise was broken (Am. Compl. ¶¶ 21-31, 66-70, 96-98). As these cases show, courts evaluating such claims consider (1) whether the personal information at issue is of the type that is protected by the constitutional right and (2) whether there was a breach of the promise of confidentiality used to obtain that information.

For example, in Fadjo v. Coon, the Fifth Circuit recognized the right discussed in Whalen, which it alternatively called the "right to confidentiality," and ruled that the plaintiff sufficiently alleged a claim based on the right. See 633 F.2d 1172, 1175 (5th Cir. 1981). In Fadjo, the state subpoenaed testimony from the plaintiff concerning "the most private details of his life," which plaintiff provided on the assurance that his testimony was "absolutely privileged" under state law and that the "contents of his testimony would be revealed to no one." Id. at 1174. The state then disclosed that information to various third parties. Id.

The Fifth Circuit noted that "[r]ecent decisions of the Supreme Court and of this circuit indicate that the right to privacy consists of two interrelated strands: 'One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.'" Id. at 1175 (quoting Whalen, 429 U.S. at 599-600). "Both strands may be understood as aspects of the protection which the privacy right affords to individual autonomy and identity. The first strand, however, described by this circuit as 'the right to confidentiality,' is broader in some respects." Id.

The court concluded that plaintiff's claim was based upon the "right to confidentiality." Id. It took as true the plaintiff's allegation that the information at issue concerned "the most private details of his life." Id. at 1174. It then concluded that plaintiff's claim was adequately pled for purpose of a motion to dismiss because "the state may have invaded [plaintiff's] privacy in revealing it to [third parties]." Id. at 1175 (noting, alternatively, that the state might have violated plaintiff's privacy rights by compelling testimony on private matters without a "legitimate and proper" aim). Accord James v. Douglas, 941 F.2d 1539, 1543-44 & n.8 (11th Cir. 1991) (embracing Fadjo and ruling that complaint sufficiently alleged a violation of a "clearly established constitutional right"—the right of privacy discussed in Whalen—where it alleged that police allowed unauthorized individuals to view of sex tape of plaintiff and his wife seized as evidence).

In Eagle v. Morgan, the Eighth Circuit demonstrated a similar understanding of the constitutional right to informational privacy. In Eagle, local

law enforcement officials disclosed an individual's prior guilty plea at a city council meeting. 88 F.3d 620, 624-25 (8th Cir. 1996). The individual sued, alleging, among other claims, breach of his constitutional right to privacy. Id. The Eighth Circuit entertained his claim, noting its view that "[t]his protection against public dissemination of information is limited and extends only to highly personal matters representing 'the most intimate aspects of human affairs.'" Id. at 625.

In the court's view, to violate the constitutional right (1) the information disclosed must be inherently private and intimate information of the type historically protected in constitutional jurisprudence, such as information about one's spouse learned or observed through marriage, medical information, and certain financial information; and (2) the disclosure "must be either a shocking degradation or an egregious humiliation of her to further some specific state interest, or a flagrant breach of a pledge of confidentiality which was instrumental in obtaining the personal information." Id. To determine whether this standard was satisfied, the court "examine[d] the nature of the material opened to public view to assess whether the person had a legitimate expectation that the information would remain confidential while in the state's possession." Id. It concluded that plaintiff failed to state a claim because the prior guilty plea was made in open court and thus public information. Id. at 625-26.

The Tenth Circuit's decision in Sheets v. Salt Lake County used a similar method of analysis. In Sheets, the plaintiff turned over the private diary of his murdered wife to police investigating her murder. 45 F.3d 1383, 1386 (10th Cir.

1995). He did so after one of the investigating detectives assured him that "the diary would remain confidential." Id. Copies of the diary were distributed to detectives and investigators on the case, one of whom allegedly shared photocopies of the diary and notes on the diary's contents with an author. Id. The author published a book about the murder containing direct quotations from the diary. Id.

The Tenth Circuit, after endorsing Whalen's view on the different interests protected by the constitutional right to privacy, explained that "due process . . . implies an assurance of confidentiality with respect to certain forms of personal information possessed by the state." Id. at 1387. It then discussed the factors used to assess whether the constitutional right to informational privacy was violated. Id. The Tenth Circuit explained that (1) "[i]nformation falls within the ambit of constitutional protection when an individual has a 'legitimate expectation . . . that it will remain confidential while in the state's possession.'"; and (2) the "legitimacy of this expectation depends, 'at least in part, upon the intimate or otherwise personal nature of the material which the state possesses'"). Id.

Using this framework, the Tenth Circuit ruled that the information at issue—plaintiff's wife's "written perceptions of their marriage"—was protected by the constitutional right to informational privacy and that there was sufficient basis for a jury to find that the right was violated. Id. at 1388-89 (affirming district court's denial of defendant's motion for judgment as a matter of law). The Tenth Circuit concluded that, although the relevant diary entries "were not extremely sensitive in nature" or "particularly controversial or embarrassing," they included

information that a jury could find "was both intimate and personal" to the plaintiff. Id. at 1388 ("[I]nformation need not be embarrassing to be personal and whether it is sufficiently personal to be protected is, in this case, a legitimate question for the jury."). The court further concluded that testimony supported the view that plaintiff had a legitimate expectation that the state would maintain the confidentiality of the personal information disclosed to it. Id. (concluding that "there was ample evidence for a jury to conclude that [plaintiff] legitimately expected his wife's diary to remain confidential while in the hands of the police").

Though the cases discussed above involve allegations of affirmative government disclosure of inherently personal information, the two-part test that they use should apply equally to claims that the government failed to safeguard such information provided to it on the promise of confidentiality. That is because, contrary to the government's assertion (Mot. at 20, 22-25), OPM had (and continues to have) an affirmative duty to protect the data entrusted to it. That affirmative duty is grounded in the constitutional right to informational privacy itself, which, as discussed above, courts have concluded is implicated when the government fails to maintain the confidentiality of inherently personal information provided to it on the promise of confidentiality. And, as the amended complaint alleges, that duty is further grounded in FISMA and the confidentiality clauses in the background investigation forms completed by NTEU Plaintiffs. Am. Compl. ¶¶ 36-37 (discussing FISMA obligations), 67-70 (noting background investigation forms state

that "[t]he information you give us is for the purpose of determining your suitability for Federal employment; we will protect it from unauthorized disclosure . . .").

Contrary to OPM's assertion (Mot. at 22-25), this affirmative duty is in accord with substantive due process principles. As one scholar has explained,

> [w]hen the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has 'by the affirmative exercise of its power' taken the data and 'so restrain[ed]' it that the original owner is unable to exert any control whatsoever over how the government stores or secures it. The government's 'affirmative duty to protect' the data 'arises . . . from the limitation which it has imposed on his freedom to act on his own behalf' to keep the data secure.

A. Michael Froomkin, Government Data Breaches, 24 Berkley Tech. L. J. 1019, 1049 (2009) (hereinafter Froomkin) (distinguishing government data breach from facts in DeShaney v. Winnebago Cnty. Dep't of Soc. Servs., 489 U.S. 189 (1989)).

Here, OPM took possession of the intimate personal information of NTEU members—which it required to be provided as a condition of employment—and explicitly promised that it would keep the information confidential (Am. Compl. ¶¶ 60-70, 96). OPM alone determined how to protect that information, rendering the "original owners" of the information, NTEU's members, powerless in terms of securing it. See Froomkin, 24 Berkley Tech. L. J. at 1049. OPM's nearly decade-long string of egregious failures to secure its information systems—failures that its own Inspector General testified "exacerbated the possibility" of a data breach (Am. Compl. ¶ 56)—were no different than the government actions in the cases discussed

above. As was true in those cases, OPM breached its affirmative duty to keep inherently personal information confidential (id. ¶¶ 96-98).

OPM's suggestion that the Privacy Act's requirements that the federal government protect personal data "allay" any potential constitutional concerns is unfounded. Mot. at 20-21. The Privacy Act cannot and does not supplant the constitutional right to informational privacy. Whalen, moreover, explicitly left open the possibility that an "unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain [adequate] security provisions" could be held to violate the constitutional right to informational privacy, notwithstanding any "concomitant statutory or regulatory duty to avoid unwarranted disclosures." See 429 U.S. at 605-06.

In sum, courts of appeals have consistently used the analysis described above to assess claims based on a constitutional right to informational privacy that arise after a disclosure has been made to the government. As shown below, using this framework, NTEU Plaintiffs have sufficiently alleged their claim.

C. NTEU Plaintiffs Sufficiently Allege That OPM's Databases Housed NTEU Members' Constitutionally Protected Information.

Because "the exact boundaries of this right are, to say the least, unclear" (Eagle, 88 F.2d at 625), there is no complete catalog of the types of personal information that are protected by the constitutional right to informational privacy. See Fraternal Order of Police, Lodge 5 v. City of Philadelphia, 812 F.2d 105, 116 (3d Cir. 1987) ("When the information is inherently private, it is entitled to protection."). Jurisprudence on the constitutional right to informational privacy

nonetheless indicates that, at a minimum, the following types of personal information—which were provided by NTEU members to OPM, which, in turn, maintained the information on the databases that were breached (see Am. Compl. ¶¶ 15, 16, 18-19, 21-31, 34-35, 66)—are generally protected by the right:

1. Information about one's spouse acquired through marriage;[9]
2. Financial information;[10]
3. Medical information;[11] and
4. Social Security Numbers.[12]

Plaintiffs Gambardella, Howell, and Ortino were among the NTEU members who provided these types of intimate personal information to OPM, which, in turn, stored it on its information systems. Am. Compl. ¶ 66. They, like other NTEU members, provided OPM with completed standard background investigation forms that required them to provide among other things, medical information (including

---

[9] See, e.g., Sheets, 45 F.3d at 1387-89 ("We find that information conveyed to one's spouse or that one's spouse has observed about one's character, marriage, finances, and business to be personal in nature and subject to a reasonable expectation of privacy."). Accord Eagle, 88 F.3d at 625.

[10] See, e.g., Fraternal Order of Police, 812 F.2d at 115 (ruling financial information is protected and assessing government need); Barry, 712 F.2d at 1559 (same).

[11] See, e.g., Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998) ("The constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality.").

[12] See, e.g., Ferm, 194 F.3d at 958-60 ("[T]he indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses, may implicate the constitutional right to informational privacy."); Arakawa v. Sakata, 133 F. Supp. 2d 1223, 1228-29 (D. Haw. 2001) ("[T]here is a constitutional right to privacy in the information released about Plaintiff in this case, specifically his SSN.").

mental health information), marital information, any history of illegal drug use, and also required them to provide their Social Security Numbers. Id. ¶¶ 21-31, 66. These documents further require employees to execute an "Authorization for Release of Information" that allows background investigators to obtain "any information" relating to the individual's "activities" from any individual, employer, credit bureau, retail business establishment, or any "other sources of information." Id. ¶¶ 22, 25, 30.

In addition to the categories of constitutionally protected personal information listed above, there are others types of personal information provided or released to OPM by NTEU members that might likewise be held, at summary judgment or after a trial on the merits, to be protected by the constitutional right—e.g., inherently private information about relatives, close friends, or other personal relationships (see id. ¶¶ 6-8, 21-31 (noting that Plaintiff Gambardella, for example, was required to submit relatives' immigration and passport numbers)). But, for present purposes, the list above is sufficient to show that NTEU Plaintiffs have sufficiently alleged that every NTEU member who provided personal information to OPM—whether that information was a Social Security Number or the full array of information that would be included in a standard background investigation file—provided OPM with constitutionally protected information.

D. NTEU Plaintiffs Sufficiently Allege that OPM's Failure to Safeguard the Protected Information, Leading to Its Taking, Violated the Right.

The complaint alleges that OPM breached its explicit promise to keep NTEU members' inherently private information—including information of the type that is

historically protected by the Constitution (Am. Compl. ¶¶ 21-31)—confidential. Id. ¶¶ 66-70, 96-98. It asserts, in particular, that OPM's failed to follow recommendations from its Inspector General for nearly a decade, creating an environment in which inherently personal information provided by NTEU members was vulnerable to the unauthorized taking of personal information that OPM revealed in 2015. Id. ¶¶ 36-57. Those allegations are sufficient to state a claim. See Fadjo, 633 F.2d at 1175 (assessing whether personal information at issue was protected by the right and whether there was a breach of a promise of confidentiality used to obtain that information); James, 941 F.2d at 1544 (same); Sheets, 45 F.3d at 1387 (same); Eagle, 88 F.3d at 625 (same).

For years leading up to the breaches announced in June 2015, OPM's OIG alerted OPM to several serious deficiencies in its information technology security programs and practices. Am. Compl. ¶¶ 41, 43. OPM's Inspector General, Patrick McFarland, testified that OPM's failure to update its cybersecurity "without question . . . exacerbated the possibility" of a breach. Id. ¶ 56. OPM Assistant Inspector General for Audits, Michael R. Esser, testified that OPM's "long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches" announced in June 2015. Id. ¶ 54. In particular, Mr. Esser highlighted the following security deficiencies known to—and ignored by—OPM:

- OPM's deficient information security governance constituted a "material weakness," which prohibited the adequate protection of data for fiscal years

2007 through 2013. It remained "fragmented and therefore inherently difficult to protect" during fiscal year 2014. Id. ¶ 44.

- In defiance of OMB requirements, eleven OPM systems were operating without a valid "authorization" (a comprehensive assessment that ensures a system meets applicable security standards) in 2014. Id. ¶¶ 45-46. OPM's OIG recommended that OPM shut down the systems, but it did not. Id.
- OPM did not maintain an accurate centralized inventory of all of its servers and databases, as federal guidelines require, and thus could not properly audit activities associated with those servers and databases. Id. ¶ 49.
- As of 2014, some of OPM's regular system vulnerability scans "were not working correctly because the tools did not have the proper credentials" and some servers were not scanned at all. Id. ¶ 48.
- Despite OMB requirements, "none of the agency's major applications required [personal identity verification] authentication." Id. ¶ 50. Nor did OPM follow the basic cybersecurity practice of encrypting its data. Id. ¶ 51-52.

Despite these known and sustained deficiencies, OPM told current and prospective federal employees who were required to submit inherently personal information to it that it would "protect [the data] from unauthorized disclosure." Id. ¶¶ 67-70. See id. at ¶ 57 ("We're a wonderful poster child of how bad it can be if you don't do the right thing," Clifton Triplett, OPM's senior cybersecurity advisor, remarked while reflecting back on the OPM data breaches). NTEU Plaintiffs' allegations concerning OPM's failures to protect the types of information found to be

protected by the constitutional right to informational privacy—information that it promised to keep confidential (id. ¶¶ 66-70)—thus state a plausible claim for relief.

That is true even if this Court concludes that OPM must evince reckless or deliberate indifference to the constitutional right to informational privacy. As OPM acknowledges (Mot. at 26), such indifference "may shock the conscience sufficiently to violate due process." See Smith v. District of Columbia, 413 F.3d 86, 93, 101-104 (D.C. Cir. 2005) (discussing evidence that could serve as basis for conclusion that the government acted "reckless[ly]" and concluding that sufficient evidence supported jury's verdict on substantive due process claim). The reckless or deliberate indifference standard governs in the substantive due process context where the government has custody of an individual. See id. at 93-94 (equating "primary legal control" to "legal responsibility" for care). The standard applies here, where the government has taken custody of inherently personal information—which federal public servants must surrender to it (Am. Compl. ¶ 96)—and has complete discretion in how it protects (or does not protect) that information. See Froomkin, 24 Berkley Tech. L. J. at 1049.

Drawing all reasonable inferences in NTEU Plaintiffs' favor and accepting their allegations as true, their complaint sufficiently states a claim against OPM. OPM's conscious and continued failure to safeguard its databases, noted above, showed a reckless indifference to its obligation to protect the information's confidentiality. Am. Compl. ¶¶ 92-97. NTEU Plaintiffs should thus be given the chance to prove that (1) they provided inherently private information to OPM on the

promise of confidentiality; and (2) OPM breached that promise through its sustained and reckless failure to safeguard its databases.

III. Sovereign Immunity Does Not Bar The Relief Sought.

While OPM acknowledges that NTEU Plaintiffs "exclusively seek declaratory and prospective injunctive relief" (Mot. at 6), it nonetheless argues that sovereign immunity bars the NTEU Plaintiffs' request for lifetime credit monitoring and identity theft protection for its members. Mot. at 27-28. That request, however, is equitable (see Mot. at 6) and aims to restore the sense of security that NTEU Plaintiffs lost when their inherently personal information was taken by hackers exploiting OPM's recklessly deficient database security.

This Court has broad authority to award equitable relief (Cobell v. Norton, 240 F.3d 1081, 1108 (D.C. Cir. 2001)), and sovereign immunity concerns do not divest this Court of that authority. "Flexibility rather than rigidity" is the essence of equity jurisdiction. See Weinberger v. Romero-Barcelo, 456 U.S. 305, 312 (1982)) ("The essence of equity jurisdiction has been the power . . . to do equity and to mould each decree to the necessities of the particular case."). Equitable relief often involves some cost, but that does not make such relief "damages." See Cigna Corp. v. Amara, 563 U.S. 421, 422, 441 (2011) (ruling district court order requiring pension plan administrator to issue payments to retired beneficiaries owed money under pension plan was equitable relief because "[e]quity courts possessed the power to provide relief in the form of monetary 'compensation' for a loss resulting from a trustee's breach of duty").

NTEU Plaintiffs' request for lifetime credit monitoring and identity theft protection to address their injuries resulting from OPM's breach of its duty to keep their personal information secure is thus equitable, even if it involves some cost. See, e.g., Vietnam Veterans of Am. v. CIA, 288 F.R.D. 192, 207 (N.D. Cal. 2012) (awarding plaintiffs lifetime healthcare as an equitable remedy because their injuries, which were continuing in nature, could not be fully remedied by money damages); New York v. Heckler, 578 F. Supp. 1109, 1125 (E.D.N.Y. 1984) (allowing, as injunctive relief, interim payments to Social Security recipients until a proper determination of their eligibility could be made). OPM's sovereign immunity argument should thus be rejected.

CONCLUSION

For the foregoing reasons, OPM's motion to dismiss should be denied. NTEU Plaintiffs respectfully request oral argument on the motion. See Local Civ. R. 7(f).

Respectfully submitted,

Gregory O'Duden
Larry J. Adkins

/s/Paras N. Shah
Paras N. Shah
Allison C. Giles
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org
Counsel for Plaintiffs

Of Counsel:

Leon O. Dayan
Devki K. Virk
BREDHOFF & KAISER PLLC
805 15th Street N.W.
Suite 1000
Washington, D.C. 20005
Tel: (202) 842-2600
Email: ldayan@bredhoff.com
Email: dvirk@bredhoff.com
Counsel for Plaintiffs

July 27, 2016