UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

MEMORANDUM OPINION

INTRODUCTION

In June of 2015, millions of unsuspecting federal employees sat down at their computers, opened up their email, and received some very disconcerting news.

> I am writing to inform you that the U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have exposed your personal information.

Over time, OPM revealed that data breaches at the agency and at one of its contractors affected more than twenty-one million people, and that the stolen information included such sensitive data as names, birthdates, current and former addresses, and Social Security numbers. After those announcements, a number of plaintiffs filed separate lawsuits in courts across the country, and they were consolidated into two complaints in the multidistrict action assigned to this Court.

The first complaint is a class action lawsuit filed by thirty-eight individuals and a union, the American Federation of Government Employees ("AFGE"). *See* Consolidated Amended Complaint [Dkt. # 63] ("CAC"). Plaintiffs allege that the breaches resulted from gross negligence on the part of officials entrusted with the responsibility of protecting the private details that job seekers submit to OPM in connection with the background investigations they are required to

undergo. They have sued on behalf of the 21.5 million current and former federal employees, job applicants, contractors, and relatives whose information was compromised, and they seek statutory damages under the Privacy Act, contract damages under the Little Tucker Act, and declaratory and injunctive relief under the Administrative Procedure Act. These plaintiffs have also sued KeyPoint Government Solutions, a government contractor that performed background investigations for OPM. KeyPoint's computer systems were also breached, and plaintiffs seek damages from the company under multiple federal and state statutory and common law theories. Defendants have moved to dismiss the entire case on the grounds that plaintiffs lack standing to bring it, the claims are barred by sovereign immunity, and the factual allegations are not sufficient to state valid claims under any of the statutes or common law theories plaintiffs have invoked.

The second complaint before the Court was filed by three individuals and the National Treasury Employees Union ("NTEU"). Am. Compl. [Dkt. # 75] ("NTEU Compl."). These plaintiffs sued the OPM Acting Director only, and they claim that their constitutional right to informational privacy was violated. Defendant has moved to dismiss that case as well, on both standing grounds and the basis that the plaintiffs have failed to allege a constitutional violation that is recognized by the courts.

The OPM breaches have been the subject of considerable public interest and multiple Congressional hearings and reports. The fact that the breaches occurred is not disputed, and the identities of the individuals whose information was compromised are known. There is no doubt that something bad happened, and many people are understandably chagrined and concerned. In these lawsuits, plaintiffs seek to demonstrate that the agency's failures were willful – that the defendants were on notice that hackers regularly targeted their systems, but they failed to design

and maintain adequate safeguards. Plaintiffs also contend that their sensitive information remains subject to a continuing risk of additional exposure due to an ongoing failure to secure it.

This opinion will not get into the merits of those contentions. At this stage of the proceedings, the Court is required to accept all of plaintiffs' factual assertions as true, and nothing that follows should be read as any indication of the Court's view of the strength of plaintiffs' troubling allegations.

Before the parties can explore the facts, though, the Court is required to answer a foundational question: whether plaintiffs have set forth a cause of action that a court has the power to hear. The judiciary does not operate as a freestanding advisory board that can opine about the conduct of the executive branch as a general matter or oversee how it manages its internal operations. The Court's authority is derived from Article III of the U.S. Constitution, and a federal court may only consider live cases or controversies based on events that caused actual injuries or created real threats of imminent harm to the particular individuals who brought the case. In other words, before a court may proceed to the merits of any claim, the plaintiffs must demonstrate that they have constitutional "standing" to sue. Also, a court may not entertain an action against the United States if the government has not expressly waived its sovereign immunity, that is, unless it has given its consent to be sued in that particular situation. And once a plaintiff overcomes those hurdles, he or she must state a valid legal claim.

This case implicates the constitutional limits on the Court's jurisdiction imposed by both the standing doctrine and the doctrine of sovereign immunity, and it involves unique factual circumstances. Neither the Supreme Court nor the U.S. Court of Appeals for the D.C. Circuit has held that the fact that a person's data was taken is enough by itself to create standing to sue; a plaintiff who claims an actual injury must be able to connect it to the defendant's actions, and a

person who is pointing to a threat of future harm must show that the harm is certainly impending or that the risk is substantial. The fact that this is not just a data breach case, but that it is a data breach arising out of a particular sort of cyberattack against the United States, differentiates it from the majority of the legal precedent that arises in the context of retail establishments or other financial entities. Courts in those cases often make certain assumptions about the likelihood of future harm in order to find that the elements needed to initiate a case have been satisfied. Here, the usual assumptions about why the information was stolen and what is likely to be done with it in the future do not apply and cannot fill the gap. As for those plaintiffs who allege that they have already experienced an actual misuse of their credit card numbers or personal information, they cannot tie those disparate incidents to this breach. It may well be that the Supreme Court or the D.C. Circuit will someday announce that given the potential for harm inherent in any cyberattack, breach victims automatically have standing even if the harm has yet to materialize, and even if the purpose behind the breach and the nature of any future harm have yet to be discerned. But that has not happened yet, and the Court is not empowered to expand the limits of its own authority, so it cannot find that plaintiffs have standing based on this record.

Even if the Court were inclined to anticipate that this is where the law is heading, the problem runs deeper than standing. The right to bring a claim for damages under the Privacy Act is expressly limited to those who can demonstrate that they have suffered actual economic harm as a result of the government's statutory violation. The law is clear that the statute does not create a cause of action for those who have been merely aggrieved by, or are even actively worried about, the fact that their information has been taken. Neither the Administrative Procedure Act nor the Little Tucker Act supplies a cause of action against the government to enforce its information

security obligations, and no court has expressly recognized a right to data security arising under the Constitution.

Therefore, defendants' motions to dismiss will be granted, and both cases will be dismissed in their entirety. The Court finds, applying the case law it is required to follow, that neither set of plaintiffs has pled sufficient facts to demonstrate that they have standing. Moreover, even if they had the right to enter the courthouse, they did not bring a claim with them that the Court can hear. Plaintiffs have failed to overcome the arguments that the federal defendants are immune from suit under the Privacy Act and the Administrative Procedure Act, and that KeyPoint is shielded by government contractor immunity, so the Court lacks subject matter jurisdiction to hear those claims. Moreover, the Court finds that plaintiffs have failed to state claims upon which relief can be granted. Plaintiffs seek damages for improper disclosure of information and for a failure to maintain adequate safeguards under the Privacy Act, but they have not alleged that private information was "disclosed," as opposed to stolen, and they have not alleged facts to show that their claimed injuries were the result of the agency's failures. Plaintiffs have not stated a claim for breach of contract under the Little Tucker Act since they have not shown that OPM entered into a contract with them or that any contract was breached, and they have not alleged any violation of the United States Constitution.

TABLE OF CONTENTS

FACTUAL BACKGROUND 7

I. The Data Breaches 7

II. The Targeted Systems and Compromised Information 8

III. OPM's Knowledge of the Deficiencies and Response to the Breaches 9

IV. Plaintiffs' Alleged Harm 111

A. Actual Identity Theft or Credit Card Fraud 11

B. Risk of Future Identity Theft and Other Harm Associated with that Risk 12

PROCEDURAL HISTORY 12

STANDARD OF REVIEW 14

I. Lack of Subject Matter Jurisdiction 14

II. Failure to State a Claim 16

ANALYSIS 17

I. Plaintiffs Do Not Have Standing. 17

A. Legal Framework 18

1. Individual Standing 18

2. Organizational Standing 19

B. Plaintiffs have Failed to Show that They have Article III Standing 20

1. Injury in Fact 21

a. Theft of Private Information Without More 21

b. Actual Identity Theft or Fraudulent Credit Card Activity 32

c. Future Identity Theft and Other Future Harms 35

2. Causation 48

II. Plaintiffs' Claims Cannot Proceed. 53

A. Claims Against OPM 53

1. Plaintiffs' Privacy Act claims must be dismissed. 53

a. All but two CAC plaintiffs fail to plead actual damages, and therefore the Court lacks subject matter jurisdiction to hear their claims. 53

b. The disclosure provision claim fails because OPM did not intentionally or willfully disclose plaintiffs' information within the meaning of the Act. 55

c. While plaintiffs have alleged a willful violation of the safeguards provision of the Privacy Act, their claim fails because they do not allege sufficient facts to show that their injuries were "a result of" OPM's conduct. 56

2. Plaintiffs fail to state a claim under the Little Tucker Act. 58

3. The Court lacks subject matter jurisdiction to hear plaintiffs' claim under the APA. 60

4. The NTEU plaintiffs fail to state a constitutional claim. 622

B. Claims Against KeyPoint 67

1. KeyPoint has derivative immunity because it was a government contractor. 68

2. Plaintiffs do not adequately identify a portion of KeyPoint's contract with OPM that KeyPoint breached. 69

3. Even if KeyPoint acted negligently, it did not lose its sovereign immunity. 71

C. Claims against both defendants for declaratory judgment and injunctive relief will be dismissed for lack of subject matter jurisdiction. 73

CONCLUSION 73

FACTUAL BACKGROUND

Defendant OPM is a federal agency that handles portions of the federal employee recruitment process. CAC ¶ 52; NTEU Compl. ¶¶ 10–11.[1] Defendant KeyPoint Government Solutions is a private contractor that conducts background investigations and security clearance checks on behalf of OPM. CAC ¶ 53.

I. The Data Breaches

The CAC plaintiffs allege that four breaches occurred in 2013 and 2014.

1 The NTEU complaint named OPM's Acting Director as the defendant in that case but sued her solely in her official capacity. NTEU Compl. ¶ 9. The Court will refer to the federal defendants named in the two complaints collectively as "OPM."

- On November 1, 2013, hackers "infiltrated" OPM's systems and stole "security system documents and electronic manuals" about the agency's systems, although no individual personal information was stolen. CAC ¶ 125; *see also* CAC ¶ 3.

- About a month later, in about December 2013, KeyPoint experienced a breach. "[A]n unknown person or persons obtained the user log-in credentials of a KeyPoint employee," and the credentials were used to "steal the personnel records of tens of thousands of Department of Homeland Security employees" from KeyPoint's systems. CAC ¶ 4.

- On May 7, 2014, hackers used "stolen KeyPoint credentials" to access OPM's network and install malware, creating "a conduit through which data could be exfiltrated." CAC ¶ 127. This breach "resulted in the theft of nearly 21.5 million background investigation records," which included "questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information of Class members." CAC ¶ 129; *see also* NTEU Compl. ¶ 19.

- Finally, "[n]o later than October 2014," hackers attacked "OPM systems maintained in an Interior Department shared-services data center." CAC ¶ 131; *see also* NTEU Compl. ¶ 14. Hackers "use[d] the stolen KeyPoint credentials to access systems within OPM's network at will" and maintained access to OPM's network for "several months," removing "millions of personnel records," resulting in "the loss of approximately 4.2 million federal employees' personnel files." CAC ¶¶ 131, 133.

II. The Targeted Systems and Compromised Information

The CAC plaintiffs allege that the nature and scope of the data breaches "indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use." CAC ¶¶ 117, 128, 132. Both complaints allege that the cyberattacks removed data from OPM computer systems and databases, including OPM's Electronic Official Personnel Folder system and the Central Verification System. *See* CAC ¶¶ 64–65, 74, 130; NTEU Compl. ¶¶ 10–12 (describing relevant OPM systems).

The Electronic Official Personnel Folder system stores personnel files of federal employees. CAC ¶¶ 74, 130. These files include "birth certificates, job performance reports, resumes, school transcripts, military service records, employment history and benefits, and job applications that contain Social Security numbers and birthdates." CAC ¶ 74; NTEU Compl. ¶ 10.

The Central Verification System "contains most background and security clearance check information," including information from the three forms – Standard Form ("SF") 85, SF 85P, and SF 86 – that applicants for federal positions and security clearances must complete.[2] CAC ¶¶ 66, 69, 70. This system also contains information on security clearances, investigations, suitability determinations, background checks for those seeking access to federal facilities, and polygraph data. CAC ¶¶ 72, 73; NTEU Compl. ¶ 12.

III. OPM's Knowledge of the Deficiencies and Response to the Breaches

Both plaintiff groups allege that OPM "knew for several years" before the breaches that its "information security governance and management protocols contained material weaknesses that posed a significant threat to its systems." CAC ¶ 90; NTEU Compl. at 3 (alleging OPM had been "on notice of serious flaws in its data system security"). The Consolidated Amended Complaint states that the OPM Inspector General's annual audits of cybersecurity from 2007 to the present "found that OPM's information security policies and practices suffered from material weaknesses" that "pose an immediate risk to the security of assets or operations." CAC ¶¶ 81, 84, 86–88; NTEU Compl. at 3 (alleging the Inspector General's office had "identified numerous significant deficiencies, including deficiencies related to OPM's decentralized security governance structure, its failure to ensure that its information technology systems met applicable security standards, and

2 The federal government uses SF 85 for applicants seeking non-sensitive federal government or contractor positions and SF 85P for applicants seeking "public trust" federal government or contractor positions. CAC ¶¶ 69–70. It requires individuals who will need security clearances to complete the SF 86. CAC ¶ 66. SF 86 is a 127-page form and, according to the CAC, it seeks information about "applicants' psychological and emotional health history, police records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants." CAC ¶ 67; *see also* NTEU Compl. ¶ 29.

its failure to ensure that adequate technical security controls were in place for all servers and databases").

After learning of the breaches, OPM issued a series of announcements to the public and affected individuals. With each revelation, the reported scope of the breach and the number of people affected increased.

On April 27, 2015, OPM notified "more than 48,000 federal employees that their personal information might have been exposed in the KeyPoint Breach." CAC ¶ 120. On June 4, 2015, it announced that it had experienced a data breach that "resulted in the exposure and theft of the [government investigation information] of approximately 4.2 million current, former, and prospective federal employees and contractors." CAC ¶ 138. On June 12, 2015, OPM acknowledged that the scope of breach was broader than previously disclosed and that "as many as 14 million current, former, and prospective federal employees and contractors" were affected. CAC ¶ 139. On July 9, 2015, OPM announced that the information "of approximately 21.5 million people had been exposed and stolen in the May 2014 breach," including the theft of 1.1 million fingerprints. CAC ¶ 140. Of the 21.5 million people affected, 19.7 million had undergone background checks. The other 1.8 million records concerned "mostly job applicants' spouses, children, and other cohabitants." CAC ¶ 140. On September 23, 2015, OPM announced that not 1.1 million, but approximately 5.6 million, fingerprints had been stolen. CAC ¶ 141.

The agency notified each individual whose private information had been compromised and offered free identity theft protection services at "a combined cost of approximately $154 million . . . for either 18 months or three years, depending on the amount and sensitivity of the compromised [information]." CAC ¶¶ 148, 150.

IV. Plaintiffs' Alleged Harm

The CAC plaintiffs allege that each of the thirty-eight named plaintiffs submitted sensitive personal information to the federal government that was compromised in the breaches. *See* CAC ¶¶ 10, 13–50; *see also* CAC ¶ 1. The NTEU plaintiffs allege that the three named plaintiffs and an unknown number of NTEU members were "identified by OPM as having been affected by the breaches." NTEU Compl. ¶ 59. Plaintiffs assert that the data breaches occurred as a result of defendants' failure to secure their systems, CAC ¶ 1, and that all of the putative class members are subject to a continuing risk of additional exposure since that failure is ongoing. CAC ¶ 7. The complaints allege that plaintiffs have sustained and will continue to sustain "economic loss and other harm," CAC ¶ 163; that they have suffered "stress," CAC ¶¶ 13, 18, 19, 22–25, 28, 30–31, 35, 37, 42–44, 46, 50; or a loss to their "sense of security," NTEU Compl. ¶ 78; and that they face an increased risk of expending time and money dealing with such consequences as identity theft and fraud in the future. CAC ¶ 163.

The complaints contain a range of allegations concerning the nature of the particular harm suffered by class members.

A. Actual Identity Theft or Credit Card Fraud

A number of plaintiffs allege that they have experienced actual identity theft or credit card fraud.

- Fourteen CAC plaintiffs and one of the three NTEU plaintiffs allege that at some point after they were informed of the breaches, they learned that unauthorized charges had been made to their existing credit card accounts or that fraudulent accounts were opened in their names. *See* CAC ¶¶ 13, 16, 19, 22, 28–31, 38, 39, 41, 45, 49, 50; NTEU Compl. ¶ 84.

- Four CAC plaintiffs allege that they experienced unauthorized credit inquiries. CAC ¶¶ 13, 14, 29, 31.

- Six CAC plaintiffs and one NTEU plaintiff allege that fraudulent tax returns were filed in their names. CAC ¶¶ 14, 21, 24, 28, 31, 32; NTEU Compl. ¶ 79.

- Four CAC plaintiffs allege that there was some other improper use of their own or a family member's Social Security number. CAC ¶¶ 14, 17, 41, 50.

B. Risk of Future Identity Theft and Other Harm Associated with that Risk

Both sets of plaintiffs claim that they have suffered harm as result of the breaches because they face an increased risk of identity theft in the future. CAC ¶¶ 7, 210; NTEU Compl. ¶ 92. Nearly all of the named CAC plaintiffs – thirty-four out of thirty-eight – allege that after learning about the breaches, they devoted some time and effort to preventing future identity theft. *See, e.g.*, CAC ¶¶ 13–22, 25–34, 36–44, 46–50 (alleging that exposure to the breach caused plaintiffs to review their financial accounts or credit reports with greater frequency, or that they placed freezes on their credit). Of those plaintiffs, seven allege that they spent money to purchased credit monitoring and protection services or incurred other expenses to prevent future identity theft. *See, e.g.*, CAC ¶¶ 17, 21, 25, 34, 41. And numerous plaintiffs allege that they "suffer stress" due to their concerns about future identity theft or a sense of vulnerability to some other harm. *See* CAC ¶¶ 18–19, 22–25, 28, 35, 37, 43–44 (expressing concerns for their safety or the safety of their family members); CAC ¶¶ 18–30, 43, 46 (expressing concern about an inability to obtain a security clearance in the future); CAC ¶¶ 19, 23–24, 42–44 (expressing fear about future identity theft); CAC ¶¶ 19, 31, 50 (alleging "stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future"); *see also* NTEU Compl. ¶ 94 (expressing anxiety over the effect the data breaches will have on them, their families, friends, and other associates).

PROCEDURAL HISTORY

A number of lawsuits were filed around the country after the data breaches at OPM and KeyPoint were announced. The United States Judicial Panel on Multidistrict Litigation transferred all actions that were pending elsewhere to this Court for coordinated or consolidated proceedings

pursuant to 28 U.S.C. § 1407 [Dkt. # 1], and plaintiffs filed two amended complaints, which are the operative documents in this matter. *See* Order (Dec. 15, 2015) [Dkt. # 19].

The plaintiffs in the Consolidated Amended Complaint[3] assert that OPM violated the Privacy Act, the Little Tucker Act, and the Administrative Procedure Act ("APA"), and that KeyPoint is liable for negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and various state statutes governing unfair and deceptive trade practices and data security. CAC ¶¶ 175–275. They seek declaratory and injunctive relief against both defendants. CAC at 75–76 (Prayer for Relief).

OPM and KeyPoint each filed motions to dismiss the CAC, arguing that the Court lacks subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) because plaintiffs do not have standing and defendants are shielded by sovereign immunity, and that plaintiffs failed to state a claim under Rule 12(b)(6). *See* KeyPoint's Mot. to Dismiss CAC & Mem. of Law in Supp. [Dkt. # 70] ("KeyPoint Mem."), Fed. Def.'s Mot. to Dismiss CAC and Mem. of P. & A. in Supp. [Dkt. # 72] ("OPM's Mem."); Pls.' Consol. Opp. to Defs.' Mots. To Dismiss [Dkt. # 82] ("CAC Pls.' Opp."); KeyPoint's Reply [Dkt. # 86]; Fed. Def.'s Reply [Dkt. # 87].

The NTEU plaintiffs assert a single claim against the Acting Director of OPM, alleging that the agency violated their constitutional right to informational privacy. NTEU Compl. ¶¶ 95–98. They seek declaratory and injunctive relief. NTEU Compl. at 34–35 (Request for Relief).

3 The CAC defines the class to include current, former, and prospective federal government employees and contractors, their family members and cohabitants, whose information was compromised as a result of the data breaches, and excludes defendants' senior officers, officials, and executives and their immediate family members, and "judicial officers to whom this case is assigned and their respective staffs." CAC ¶ 165.

OPM has moved to dismiss the NTEU complaint for lack of standing and for failure to state a claim.[4] *See* Fed. Defs.' Mot. to Dismiss NTEU Compl. [Dkt. # 81]; Mem. in Supp. [Dkt. # 81-1]; NTEU Pls.' Opp. to OPM's NTEU Mot. [Dkt. # 84] ("NTEU's Opp."); Fed. Def.'s Reply Mem. in Supp. of Mot. to Dismiss [Dkt. # 91].[5]

The Court heard oral argument on the motions, and the motions are fully briefed.

STANDARD OF REVIEW

In evaluating a motion to dismiss under either Rule 12(b)(1) or 12(b)(6), 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.'" *Sparrow v. United Air Lines, Inc.*, 216 F.3d 1111, 1113 (D.C. Cir. 2000) (internal citations omitted), quoting *Schuler v. United States*, 617 F.2d 605, 608 (D.C. Cir. 1979); *see also Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011). Nevertheless, the Court need not accept inferences drawn by the plaintiff if those inferences are unsupported by facts alleged in the complaint, nor must the Court accept plaintiff's legal conclusions. *Browning v. Clinton*, 292 F.3d 235, 242 (D.C. Cir. 2002).

I. Lack of Subject Matter Jurisdiction

Under Rule 12(b)(1), the plaintiff bears the burden of establishing jurisdiction by a preponderance of the evidence. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992); *Shekoyan*

---

4 OPM also asserts that plaintiffs have failed to identify any statute that would waive sovereign immunity and enable the Court to order the agency to pay for lifetime credit monitoring. OPM's Mem. at 27–28.

5 *See also* Joint Omnibus Notice of Supp. Auth. [Dkt. # 95]; Notice of Recent Decision [Dkt. # 99]; Def. KeyPoint's Notice of Suppl. Citations [Dkt. # 102]; Pls.' Resp. to Def. KeyPoint's Notice of Suppl. Citations [Dkt. # 103]; Notice of Suppl. Auth. [Dkt. # 106], Resp. to Notice of Suppl. Auth. [Dkt. # 107], Resp. to Notice of Suppl. Auth. [Dkt. # 108], Notice of Recent Decision [Dkt. # 109], Resp. to Notice of Recent Decision [Dkt. # 110], Notice of Supp. Auth. [Dkt. # 111], NTEU Pls.' Supp. Submission [Dkt. # 112], Fed. Def. OPM's Suppl. Submission regarding *Attias v. CareFirst, Inc.* [Dkt. # 113], Def. KeyPoint's Suppl. Submission regarding *Attias v. CareFirst, Inc.* [Dkt. # 114], and Class Pls.' Suppl. Submission [Dkt. # 115].

v. Sibley Int'l Corp., 217 F. Supp. 2d 59, 63 (D.D.C. 2002). Federal courts are courts of limited jurisdiction and the law presumes that "a cause lies outside this limited jurisdiction." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *see also Gen. Motors Corp. v. EPA*, 363 F.3d 442, 448 (D.C. Cir. 2004) ("As a court of limited jurisdiction, we begin, and end, with an examination of our jurisdiction."). "[B]ecause subject-matter jurisdiction is 'an Art[icle] III as well as a statutory requirement . . . no action of the parties can confer subject-matter jurisdiction upon a federal court.'" *Akinseye v. District of Columbia*, 339 F.3d 970, 971 (D.C. Cir. 2003), quoting *Ins. Corp. of Ir., Ltd. v. Compagnie des Bauxites de Guinee*, 456 U.S. 694, 702 (1982).

When considering a motion to dismiss for lack of jurisdiction, unlike when deciding a motion to dismiss under Rule 12(b)(6), the court "is not limited to the allegations of the complaint." *Hohri v. United States*, 782 F.2d 227, 241 (D.C. Cir. 1986), *vacated on other grounds*, 482 U.S. 64 (1987). Rather, "a court may consider such materials outside the pleadings as it deems appropriate to resolve the question [of] whether it has jurisdiction to hear the case." *Scolaro v. D.C. Bd. of Elections & Ethics*, 104 F. Supp. 2d 18, 22 (D.D.C. 2000), citing *Herbert v. Nat'l Acad. of Scis.*, 974 F.2d 192, 197 (D.C. Cir. 1992); *see also Jerome Stevens Pharm., Inc. v. FDA*, 402 F.3d 1249, 1253 (D.C. Cir. 2005).

Furthermore, when a government agency is the defendant, additional jurisdictional considerations apply. The United States is not amenable to suit in the federal courts absent an express waiver of sovereign immunity. *Anderson v. Carter*, 802 F.3d 4, 8 (D.C. Cir. 2015), citing *United States v. Mitchell*, 463 U.S. 206, 212 (1983). Sovereign immunity is "jurisdictional in nature." *Perry Capital LLC v. Mnuchin*, 864 F.3d 591, 619 (D.C. Cir. 2017), quoting *FDIC v. Meyer*, 510 U.S. 471, 475 (1994). When it has not been waived, sovereign immunity shields the federal government, its agencies, and federal officials acting in their official capacities from suit.

Meyer, 510 U.S. at 475 (the federal government and its agencies); *Kentucky v. Graham*, 473 U.S. 159, 166–67 (1985) (federal officials in their official capacities).

II. Failure to State a Claim

"To survive a [Rule 12(b)(6)] 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), quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In *Iqbal*, the Supreme Court reiterated the two principles underlying its decision in *Twombly*: "First, the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions," and "[s]econd, only a complaint that states a plausible claim for relief survives a motion to dismiss." *Id.* at 678–79.

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.* at 678, citing *Twombly*, 550 U.S. at 556. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*, quoting *Twombly*, 550 U.S. at 556. A pleading must offer more than "labels and conclusions" or a "formulaic recitation of the elements of a cause of action," *id.*, quoting *Twombly*, 550 U.S. at 555, and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.*, citing *Twombly*, 550 U.S. at 555.

When considering a motion to dismiss under Rule 12(b)(6), the Court is bound to construe a complaint liberally in the plaintiff's favor, and it should grant the plaintiff "the benefit of all inferences that can be derived from the facts alleged." *Kowal v. MCI Commc'ns Corp.*, 16 F.3d 1271, 1276 (D.C. Cir. 1994). Nevertheless, the Court need not accept inferences drawn by the plaintiff if those inferences are unsupported by facts alleged in the complaint, nor must the Court accept plaintiff's legal conclusions. *See id.*; *see also Browning*, 292 F.3d at 242. In ruling upon a

motion to dismiss for failure to state a claim, a court may ordinarily consider only "the facts alleged in the complaint, documents attached as exhibits or incorporated by reference in the complaint, and matters about which the Court may take judicial notice." *Gustave-Schmidt v. Chao*, 226 F. Supp. 2d 191, 196 (D.D.C. 2002), citing *EEOC v. St. Francis Xavier Parochial Sch.*, 117 F.3d 621, 624–25 (D.C. Cir. 1997).

ANALYSIS

Defendants seek to dismiss both complaints for lack of subject matter jurisdiction on the grounds that plaintiffs lack standing and that there has not been a valid waiver of sovereign immunity, and they have also moved to dismiss for failure to state a claim. Courts must determine whether they have jurisdiction to hear a case before considering whether plaintiffs have failed to state a claim. *Hancock v. Urban Outfitters*, 830 F.3d 511, 513 (D.C. Cir. 2016) ("Federal courts cannot address the merits of a case until jurisdiction – the power to decide – is established.") Accordingly, the Court will address the issue of plaintiffs' standing first.

I. Plaintiffs Do Not Have Standing.

"To state a case or controversy under Article III, a plaintiff must establish standing." *Ariz. Christian Sch. Tuition Org. v. Winn*, 563 U.S. 125, 133, citing *Allen v. Wright*, 486 U.S. 737, 751 (1984); *see also Lujan*, 504 U.S. at 560. Standing is a necessary predicate to any exercise of federal jurisdiction; if it is lacking, then the dispute is not a proper case or controversy under Article III, and federal courts have no subject matter jurisdiction to decide the case. *Dominguez v. UAL Corp.*, 666 F.3d 1359, 1361 (D.C. Cir. 2012). Plaintiffs must demonstrate standing for each claim they assert. *Daimler Chrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (holding that "our standing cases confirm that a plaintiff must demonstrate standing for each claim he seeks to press"); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 185 (2000). And each plaintiff must demonstrate standing, including in a putative class action. *See Lujan*, 504 U.S. at

563 ("The 'injury in fact' test . . . requires that the party seeking review be himself among the injured."), quoting *Sierra Club v. Morton*, 405 U.S. 727, 734 (1972); *see also Warth v. Seldin*, 422 U.S. 490, 502 (1975) (named plaintiffs in a putative class action "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent").

The party invoking federal jurisdiction bears the burden of establishing standing. *Lujan*, 504 U.S. at 561. When reviewing the standing question, the Court must be "careful not to decide the questions on the merits for or against the plaintiff, and must therefore assume that on the merits the plaintiffs would be successful in their claims." *In re Navy Chaplaincy*, 534 F.3d 756, 760 (D.C. Cir. 2008), quoting *City of Waukesha v. EPA*, 320 F.3d 228, 235 (D.C. Cir. 2003).

A. Legal Framework

To establish constitutional standing, plaintiffs must show that (1) they have suffered an "injury in fact," (2) the injury is "fairly . . . trace[able] to the challenged action of the defendant," and (3) it is "'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" *Lujan*, 504 U.S. at 560–61 (citations omitted); *see also Friends of the Earth, Inc.*, 528 U.S. at 180–81.

1. Individual Standing

Individual plaintiffs must satisfy all three of the *Lujan* elements. To allege the first element, injury in fact, plaintiffs must demonstrate that they "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), quoting *Lujan*, 504 U.S. at 560.

To be "concrete," the injury "must actually exist," meaning that it is real, and not abstract, although concreteness is "not . . . necessarily synonymous with 'tangible.'" *Id.* at 1548–49. And

to be "particularized," the injury must affect a plaintiff "in a personal and individual way." *Id.* at 1548, quoting *Lujan*, 504 U.S. at 560 n.1.

Further, the injury must be "actual," or it must be "imminent" – that is, the "threatened injury must be certainly impending to constitute injury in fact." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410 (2013); *see also Pub. Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1293 (D.C. Cir. 2007) (the injury must be "certainly impending and immediate – not remote, speculative, conjectural, or hypothetical"). Or, as the D.C. Circuit has recently pointed out, the Supreme Court has "also noted that in some cases it has 'found standing based on a substantial risk that the harm will occur.'" *Attias v. CareFirst, Inc.*, 865 F.3d 620, 626 (D.C. Cir. 2017), quoting *Clapper*, 568 U.S. at 414 n.5.

To establish the second element, and show that an injury is "fairly traceable" to a defendant's action, a plaintiff must allege a causal connection between the alleged injury and the defendant's conduct at issue. *Ctr. for Law & Educ. v. Dep't of Educ.*, 396 F.3d 1152, 1157 (D.C. Cir. 2005). The alleged harm cannot be "the result of the independent action of some third party not before the court." *Food & Water Watch v. EPA*, 5 F. Supp. 3d 62, 73 (D.D.C. 2013), quoting *Lujan*, 504 U.S. at 560–61. "But Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant." *Attias*, 865 F.3d at 629.

Finally, to be "redressable," the alleged injury must be one that a court order in favor of the plaintiff would be "likely" to address the harm. *Lujan*, 504 U.S. at 560–61.

2. Organizational Standing

The standing requirements that apply to individuals also apply to organizations, such as the two unions that are plaintiffs: AFGE and NTEU. *Nat'l Treasury Emps. Union v. United States*, 101 F.3d 1423, 1427 (D.C. Cir. 1996), citing *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 378

(1982). Organizations may assert standing on their own behalf under certain circumstances, or they may seek representational standing on behalf of their members. *Nat'l Ass'n of Home Builders v. EPA*, 667 F.3d 6, 12 (D.C. Cir. 2011).

To assert organizational standing, an organization must allege "such a 'personal stake' in the outcome of the controversy as to warrant the invocation of federal-court jurisdiction," and must show "concrete and demonstrable injury to the organization's activities – with [a] consequent drain on the organization's resources – constitut[ing] . . . more than simply a setback to the organization's abstract social interests." *Nat'l Taxpayers Union, Inc. v. United States*, 68 F.3d 1428, 1433 (D.C. Cir. 1995) (alterations in original), quoting *Havens Realty*, 455 U.S. at 378–79.

To assert representational standing on behalf of its members, an organization must show that "(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." *Nat'l Ass'n of Home Builders*, 667 F.3d at 12, quoting *Ass'n of Flight Attendants-CWA v. U.S. Dep't of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009).

B. Plaintiffs have Failed to Show that They have Article III Standing

Plaintiffs allege that some of them have incurred actual out-of-pocket expenses, that others have expended time and effort, and that others have experienced emotional distress or may be subject to identity theft or some other harm in the future. Plaintiffs also contend that all of them have suffered the injury of the breach itself. The Court is not persuaded that the factual allegations in the complaints are sufficient to establish constitutional standing.

1. Injury in Fact

a. Theft of Private Information Without More

At oral argument, counsel for the CAC plaintiffs took to the lectern to advocate a new basis for standing that had not been set forth in any prior consolidated pleading: that the release or theft of private information – as opposed to any actual or even threatened misuse of that information – is itself the injury in fact for standing purposes in a Privacy Act case. Hr'g Tr. [Dkt. # 98] at 26–28 ("I don't think you get to the question of imminence because we're not talking about a risk of future injury; the injury happened; . . . . [W]e're not premising the Court's Article III standing on a risk of future injury, we're premising it on an injury that has occurred and has been recognized at common law."). In other words, if your personal information was included in the material accessed in a data breach, you automatically have standing to bring an action predicated on a violation of the Privacy Act. *See* NTEU Compl. ¶ 76 (alleging that harm "occurred the moment that [plaintiffs'] inherently personal information . . . was taken by unauthorized intruders from OPM's databases").

While one could make a compelling argument that this would be an appropriate principle to adopt in data breach cases given the volume, sensitivity, and vulnerability of computerized private information, the Court is not writing a law review article. Therefore, it cannot ignore the fact that neither the Supreme Court nor the D.C. Circuit has embraced this categorical approach to standing to date. In the absence of authority to support plaintiffs' proposal, it is not up to the Court to expand the constitutional limitations on its jurisdiction on its own initiative, particularly when considerations of sovereign immunity and separation of powers concerns are also involved. *See Spokeo*, 136 S. Ct. at 1547 (the standing doctrine developed "to ensure that federal courts do not exceed their authority as it has been traditionally understood"). Therefore, the Court believes that it is constrained to find that plaintiffs cannot predicate standing on the basis of the breach alone.

At the hearing, plaintiffs pointed to *Doe v. Chao*, 540 U.S. 614 (2004), as support for the notion that "the release itself is the injury." Hr'g Tr. at 32. But the case does not stand for that proposition. In *Doe*, the Supreme Court held that a plaintiff must suffer actual damages to bring a claim under Privacy Act. *Id.* at 616. In the course of the opinion, the Court noted that the petitioner had argued against that interpretation; he pointed out that in subsection (g)(1) of the statute, Congress expressly granted any individual who suffered an "adverse effect" as a result of an agency's failure to comply with the Act the right to sue that agency without any further limitation. *Id.* at 624. In responding to that argument, the Court stated:

> [T]he reference in § 552a(g)(1)(D) to 'adverse effect' acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue. That is, an individual subjected to an adverse effect has injury enough to open the courthouse door, but without more has no cause of action for damages under the Privacy Act.

Id. at 624–25.

That discussion does not necessarily mean that anyone whose information was included in a data breach automatically "has injury enough to open the courthouse door;" the statutory reference to an adverse "effect" seems to imply that there is a need for individualized consequences beyond the mere fact that a release took place, and Doe himself alleged that he suffered from

emotional distress.[6] *See id.* at 617–18. And the Court in *Doe* did not purport to answer the question of whether the release of private information alone is an "adverse effect."

Plaintiffs also insisted that this issue was "specifically considered" in *In re Department of Veterans Affairs Data Theft Litigation*, No. 06-0506, 2007 WL 7621261 (D.D.C. Nov. 16, 2007) ("*VA Data Theft Litig.*"). Hr'g Tr. at 27 ("[T]he Court said yes, that's an adverse effect, that gives rise to Article III standing."); *see also* Hr'g Tr. at 27–28 ("[T]he injury occurs at that moment. And this is a precise issue that the Court looked at in the *VA Laptops* case."). It is true that the *VA Data Theft* opinion denied a motion to dismiss for lack of subject matter jurisdiction. But the court in that case did not consider at any point whether a release of data in and of itself constitutes an injury that would give rise to standing.

The VA plaintiffs did not rely on the fact of the breach as the foundation for their suit; they specifically alleged that they had suffered pecuniary and emotional harm as a result of the theft, including the cost of credit reports and credit monitoring services, and mental anguish. *VA Data Theft Litig.*, 2007 WL 7621261, at *3. The government moved to dismiss on the grounds that these allegations of harm were not tied to any particular plaintiff and that they were insufficiently

6 At another point in the hearing, one of the other attorneys for the plaintiffs pointed the Court to the dissent in *Doe*, in which Justice Ginsburg argued against the ruling by the majority that one must suffer economic loss in addition to emotional distress to advance a Privacy Act claim. Hr'g Tr. at 37. In her opinion, the Justice emphasized that "Doe has standing to sue . . . based on 'allegations that he was "torn . . . all to pieces" and "greatly concerned and worried" because of the disclosure of his Social Security number and its potentially "devastating" consequences,'" and she reasoned that the statute should call for no more for the claim to move forward. 540 U.S. at 641 (Ginsburg, J., dissenting) (quoting *Doe*, 540 U.S. at 617–18). The Justice's observation that the distraught Mr. Doe had standing does not bear on the question of whether these plaintiffs have standing by virtue of the release of their data even if they suffered no further consequences at all.

detailed. *Id.* The court simply found the general allegations of monetary harm to be sufficient,[7] and it did not predicate its decision on the mere fact that the data had gone missing. *Id.*

At the hearing, plaintiffs appeared to be drawing on the concepts underlying the Supreme Court's decision in *Spokeo* when they maintained that they had standing simply because they were the victims of a Privacy Act violation:

> As I understand the Privacy Act, it's really codifying common law privacy protection principles . . . . [T]his isn't like a procedural violation case because the harm has occurred upon the release, and the reason is that the underlying claim is rooted in the common law protection of privacy principles. And so it was recognized at common law that if your private information was made public or there was an intrusion on your right to seclusion, the injury occurs at that moment.

Hr'g Tr. at 26–28; *see Spokeo*, 136 S. Ct. at 1549. Plaintiffs acknowledged that *Spokeo* requires a would-be plaintiff to make a showing of harm, Hr'g Tr. at 28, but they maintained that the showing had been made in this case because it is inherent in the nature of the allegations.

> [I]t does cause harm . . . . [T]he harm is recognized at common law. So it's not like a situation – let's say it's a Truth in Lending Act claim and you have the right so some disclosure . . . [and] it never had any impact on you whatsoever. That's *Spokeo*. This is different. This is a common law right to the protection of your private facts. That right is infringed at the point when the release occurs. And the causation issue doesn't enter in . . . .

Hr'g Tr. at 28–29.

What plaintiffs are suggesting, then, is that the challenged action that makes the defendant liable – in this case, a failure to prevent a breach – is also the harm: the loss of the data is the whole story. But adopting that approach would collapse the standing analysis in data breach cases

7 That aspect of the *VA Data Theft* holding has limited precedential value given the subsequent Supreme Court rulings in *Clapper*, 568 U.S. 398, and *FAA v. Cooper*, 566 U.S. 284 (2012). It is true that in *Cooper*, the Supreme Court considered the requirements for a Privacy Act claim without addressing the standing question. While plaintiffs argue that means the Court was not troubled by the standing issue in that case, *see* Hr'g Tr. at 37, the opinion supplies no guiding principles to be applied here.

entirely, answering both of the injury-in-fact inquiries – is the harm actual or imminent and is it concrete and particularized? – and the causation and redressability inquiries – is the injury fairly traceable to the defendant's unlawful action and would the relief sought cure the harm? – with a single allegation: my data was involved. Adopting such a tautological approach would effectively eliminate the requirement to establish the elements of Article III standing in data breach cases brought against the government, and while the Supreme Court may be headed in that direction, it has not arrived there yet.

A close reading of the majority opinion in the *Spokeo* case reveals that the Court did not relax traditional standing requirements – if anything, *Spokeo* reaffirmed the constitutional underpinnings of the doctrine – and it stopped short of the theory plaintiffs advance here. The holding addresses only one prong of the standing analysis – concreteness – and it left critical aspects of even that issue open for further development. While the Court opined that a violation of a statute enacted to protect rights that have traditionally been recognized in our courts could give rise to a concrete injury without more in some circumstances, it cautioned that it would not do so in all circumstances. And disappointing commentators everywhere, it left the delineation of the boundary for another day. Since isolated phrases from the opinion can point in different directions when lifted out of context, it is necessary to review the opinion of the Court in some detail. But the message to be gleaned from that analysis is that the holding underscored that an injury in fact predicated on a statutory violation – even a violation of a statute intended to protect

a traditionally recognized personal right – must carry with it a risk of "real harm."[8] *Spokeo*, 136 S. Ct. at 1549.

Spokeo is a firm that conducts searches of computerized databases to supply visitors to its website with information about the people they identify. *Spokeo*, 136 S. Ct. at 1544. The plaintiff, Robins, became aware that personal information that had been disseminated about him – including his age, marital status, and employment – was incorrect, and he instituted a class action against the company for violating the Fair Credit Reporting Act. *Id.* at 1546. The district court dismissed the action on the grounds that Robins had failed to allege the necessary injury in fact, but the Ninth Circuit reversed, finding that the allegation that Robins's own statutory rights had been violated was sufficient. *Id.* The Supreme Court sent the case back, complaining that the Ninth Circuit had considered only the "particularized" portion of the requirement that an injury be "concrete and particularized," and it called for the missing half of the review. *Id.* at 1549.

The *Spokeo* analysis begins by reciting the holding in *Lujan* that "the 'irreducible constitutional minimum' of standing consists of three elements": injury in fact, traceability, and redressability, *id.* at 1547, quoting *Lujan*, 504 U.S. at 560, and that a plaintiff must allege facts demonstrating each. *Id.*, citing *Warth*, 422 U.S. at 518. The Court reiterated that "[i]njury in fact is a constitutional requirement, and 'it is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.'" *Id*. at 1547–48, quoting *Raines v. Byrd*, 52 U.S. 811, 820 n.3 (1997). The Court listed

8 If the loss of data in and of itself is not an injury in fact, then for the same reasons, plaintiffs' allegation that they are subject to a risk of another breach in the future because the security flaws have yet to be rectified, *see* CAC ¶ 7, does not allege a threat of future harm that constitutes an injury in fact.

the multiple components of the injury-in-fact element, but it went on to discuss just the particularization and concreteness requirements. *Id.* at 1548–50.

The Court repeated that "for an injury to be 'particularized,' it must affect the plaintiff in a 'personal and individual way.'" *Id.* at 1548, quoting *Lujan*, 504 U.S. at 560 n.1. But it emphasized that particularization is "not sufficient. An injury in fact must also be 'concrete.'" *Id.* ("We have made it clear time and time again that in injury in fact must be both concrete and particularized."). The opinion went on to explain that while the injury must be "'*de facto*,' that is, it must actually exist," and that it must be "'real' and not 'abstract,'" it is not necessary that the injury be tangible to be concrete. *Id.* at 1548-49 ("[W]e have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

How would one go about identifying an intangible harm that constitutes a concrete injury in fact? Writing for the Court, Justice Alito explained that "both history and the judgment of Congress play important roles." *Id.* at 1549.

> [I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. In addition, because Congress is well-positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important.

Id. (citations omitted). At the same time, the opinion cautioned that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff *automatically* satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Id.* (emphasis added).

> Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm and satisfy the injury-in-fact requirement . . . .

Id. Turning back to the other hand, Justice Alito went on:

> This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness. For example, the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure. Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient *in some circumstances* to constitute injury in fact. In other words, a plaintiff *in such a case* need not allege any additional harm beyond the one Congress has identified.

Id. (emphasis added) (emphasis and citations omitted).

Applying all of those general principles to the case before him, Justice Alito derived two conclusions: that Congress clearly intended to prevent the harm that had befallen Robins, i.e., the dissemination of false information, when it enacted the provisions that were alleged to have been violated, but that Robins could not meet the requirements of Article III standing simply by alleging a "bare procedural violation." *Id.* Since it was possible that a violation of one of the statute's procedural requirements could result in *no* harm, the case was remanded to the Ninth Circuit to address "whether the particular procedural violations alleged . . . entail a degree of risk sufficient to meet the concreteness requirement." *Id.* at 1550.

According to plaintiffs, their allegation of a statutory violation supplies a basis for standing since they suffered the harm of an intangible violation of their privacy – a harm traditionally recognized at common law that Congress specifically intended to protect when it enacted the statute in question. Hr'g Tr. at 28–29. But that is exactly what the Supreme Court found to be insufficient in *Spokeo* without a further showing that real harm, albeit even intangible harm, would

necessarily follow.[9] And the opinion was specifically limited to a consideration of the "concrete and particularized" element of an injury in fact; the Supreme Court did not hold that once a plaintiff has alleged an injury to a traditionally recognized intangible right that satisfies the concreteness requirement, there is no longer any need to establish that the harm is actual or imminent, or to satisfy the traceability or redressability requirements.

This reading of *Spokeo* is consistent with the Circuit precedent that the Court is bound to follow; the Court of Appeals emphasized in *Hancock v. Urban Outfitters* that *Spokeo* did not alter the standing requirements. "*Spokeo* held that plaintiffs must have suffered an actual (or imminent) injury that is both particularized and 'concrete . . . even in the context of a statutory violation' . . . . For that reason, a plaintiff cannot 'allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.'" *Hancock*, 830 F.3d at 514, quoting *Spokeo*, 136 S. Ct. at 1549. In *Hancock*, there was no question that each of the plaintiffs was personally involved: each had been asked to provide her zip code during the course of a credit card transaction, and that information was entered into the retailer's sales register. *Id.*

9 Plaintiffs' counsel attempted to differentiate *Spokeo* – "it's not like a situation – let's say it's a Truth in Lending Act claim and you have some right to some disclosure and you never saw the disclosure . . . it never had any impact on you whatsoever. That's *Spokeo* . . . ." – but that characterization of the case was incorrect. Hr'g Tr. at 28–29. In *Spokeo*, Justice Alito specifically found that the complained of action *did* intrude on Robins's privacy rights, and he still resisted concluding that Robins automatically had standing, finding that the violation of a statutorily imposed procedure might not necessarily carry with it a risk of real harm that would satisfy the concreteness requirement. *Spokeo*, 136 S. Ct. at 1550. Plaintiffs allege two statutory violations here. They allege a "disclosure" in violation of the Privacy Act, CAC ¶¶ 175–85, but as set forth in section II.A.1.B. below, a theft does not qualify as a "disclosure." So the core of plaintiffs' claim is that OPM failed to comply with the requirements in the statute that it "establish appropriate . . . safeguards" to protect agency records. 5 U.S.C. § 552a(e)(10). The Court is hard pressed to assess the sufficiency of allegations in the complaint that such a failure necessarily entails a degree of risk sufficient to satisfy the concreteness requirement because this basis for standing is not set forth in the complaint, plaintiffs did not advance the theory in their papers, and they assumed at oral argument that no discussion of harm was required.

at 512. But the Court was clear that the allegation of a violation of the District of Columbia's Consumer Protection Act was not enough to create an injury in fact absent any allegation of a concrete consequence:

> The Supreme Court has been clear that the legislature "cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing" . . . . Instead, an asserted injury to even a statutorily conferred right "must actually exist," and must have "affect[ed] the plaintiff in a personal and individual way."

Id. at 514,[10] quoting *Spokeo*, 136 S. Ct. at 1547–48 (citations omitted); *see also Attias*, 865 F.3d at 626–27 (Court of Appeals relied on the sufficiency of allegations of future identity theft, and not the fact of the release of the data alone, as the basis for finding standing).

Plaintiffs seemed to find support in Justice Thomas's concurring opinion in *Spokeo*, Hr'g Tr. at 28, but Justice Thomas did not address the precise situation before the Court either. In agreeing with the decision to remand, he differentiated between a suit brought by an individual to vindicate a private right, and a suit seeking to vindicate a public right – a demand that a federal agency "follow the law." *Spokeo*, 136 S. Ct. at 1552 (Thomas, J., concurring). He said that in the second instance, there needs to be some personal impact on the plaintiff, and given separation of powers concerns, Congress cannot simply authorize private plaintiffs to enforce public rights without meeting all of the constitutionally based requirements. *Id.* But he differentiated that situation from a suit like the one in *Spokeo* in which a private plaintiff was seeking to enforce his own private rights against a private party: "[i]f Congress has created a private duty owed personally to Robins to protect *his* information, then the violation of the legal duty suffices for

10 The Court observed that neither *Hancock* plaintiff had alleged any invasion of privacy, increased risk of fraud or identity theft, or pecuniary or emotional injury, but it did not specifically address the question of whether an allegation of an invasion of privacy rights alone would suffice. 830 F.3d at 514.

Article III injury in fact." *Id.* at 1554 (Thomas, J., concurring).[11] Neither alternative quite mirrors the situation of a private plaintiff suing a federal defendant to vindicate a private right.

But more important, even if one assumes that the principles reviewed by the Justices would apply equally to cases against the government, the *Spokeo* discussion arose in the context of a statute that creates a private right of action for a statutory violation without the need for a showing of harm. *See id.* at 1553 (Thomas, J, concurring) ("Congress can create new private rights and authorize private plaintiffs to sue *based simply on the violation of those private rights*. A plaintiff seeking to vindicate a statutorily created private right need not allege actual harm beyond the invasion of that private right.") (emphasis added) (citation omitted); *see also id.* at 1549 ("[T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact . . . . [A] plaintiff in such a case need not allege any *additional* harm *beyond the one Congress has identified*.") (first emphasis in original, second emphasis added).

The Privacy Act is not that sort of statute. Congress carefully limited the remedies that would be available in a Privacy Act case, and it specifically added the requirement of a showing of actual harm beyond the statutory violation and its impact on one's privacy before the government would be required to answer in Court. So even if the Court were inclined to read the tea leaves and predict that the Supreme Court will eventually find that the bare allegation that a plaintiff was a victim of a data breach, without more, is enough to create standing to sue under the Privacy Act given the privacy rights involved, the victory for plaintiffs would be a hollow one. Because notwithstanding any invasion of privacy, before the Court may pierce the shield of sovereign immunity and exercise jurisdiction, it must consider still whether the complaint

11 The Court notes that the dissenters were of the firm belief that Robins had standing. *Spokeo*, 136 S. Ct. at 1554–56 (Ginsburg, J., dissenting).

plausibly alleges that the named plaintiffs suffered the actual damages necessary to require the government to submit to a Privacy Act claim, and as set forth further below, it does not.

And finally, even if the Court were to find that there is standing to sue under the Privacy Act because Congress authorized plaintiffs to sue to vindicate their private rights in that Act, that would only confer standing to bring the Privacy Act claim. Contrary to plaintiffs' suggestion, *see* Hr'g Tr. at 30,[12] it would not open the door for plaintiffs to advance the APA claims based on OPM's violation of the Federal Information Security Management Act ("FISMA"). *See Cuno*, 547 U.S. at 352; *Friends of the Earth*, 528 U.S. at 185. Congress did not establish a private right to sue under FISMA, and there is no basis to conclude that the statutory regime protecting all systems and records across the federal government was specifically intended to vindicate individual rights that are grounded in our history or tradition.

For all of these reasons, in the Court's view, standing in this case must rise or fall on the sufficiency of the allegations of actual or future harm set forth in the complaint, and it is necessary to undertake that analysis.[13]

b. Actual Identity Theft or Fraudulent Credit Card Activity

Twenty plaintiffs allege that they have already experienced identity theft or have been the victims of financial fraud. They describe unauthorized charges made to existing accounts or accounts fraudulently opened in their names, unauthorized inquiries made concerning their credit, fraudulent tax returns filed in their names, or other improper uses of their credit card or Social

12 "I thought standing was a gatekeeping doctrine that says, Do you have a right to be in court? . . . [T]o me, once you're in court, if you read cases, courts don't go through every claim . . . in the case and analyze standing separately for each one."

13 In any event, after the D.C. Circuit issued its opinion in *Attias*, and the Court called for supplemental briefing, plaintiffs reverted back to the theory articulated in their complaint: that all plaintiffs have standing based on the risk of future harm. Class Pls.' Supp. Submission [Dkt. # 115] at 4–5.

Security numbers. CAC ¶¶ 13, 14, 16, 17, 19, 21, 24, 26, 28–32, 38, 39, 41, 45, 49, 50; NTEU Compl. ¶¶ 80–84. For example:

- Plaintiff "King-Myers provided sensitive information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, King-Myers learned that unauthorized charges of approximately $658 had been incurred on her debit card account. King-Myers has spent between 30 and 35 hours attempting to reverse these fraudulent transactions." CAC ¶ 38.

- Plaintiff Ryan Lozar provided sensitive information and received notice that his information was compromised. "Lozar thereafter learned that an unknown individual had opened a PayPal account in his name and received a $1000 cash advance. He also learned that an unidentified individual had opened a Best Buy account in his name and used it to purchase $3,500 worth of merchandise." Lozar spent many hours communicating with PayPal and Best Buy to dispute and resolve these fraudulent activities. CAC ¶ 39.

- Plaintiff Kimberly Winsor and her husband "provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, Winsor's husband learned from their bank that his debit card number had been used the make unauthorized purchases in Mississippi. On July 23, 2015, Winsor learned from their bank that her debit card had been used to make unauthorized purchases in Texas. On November 24, 2015, CSID informed Winsor that her 8 year old son's social security number had been used in California for an unknown purpose." CAC ¶ 50.[14]

Only two of these plaintiffs allege that they incurred out-of-pocket expenses related to actual identity theft. *See* CAC ¶ 22 (plaintiff "paid approximately $198 to a credit repair law firm for assistance in closing the fraudulent accounts and removing them from her credit report" and "expended approximately $50 to obtain copies of her credit report"); CAC ¶ 41 (plaintiff purchased credit repair services). None of the plaintiffs who allege that unauthorized charges were made to their accounts allege that they were held financially responsible for the charges, *see* CAC ¶¶ 13, 16, 19, 22, 28–31, 38–39, 41, 45, 49, 50; NTEU Compl. ¶ 80–84, and none who

14 The complaint does not specifically allege that the son's Social Security number was included in the "sensitive information" provided to the federal government in connection with Winsor's employment.

experienced other attempts to utilize their identity alleged that they incurred out-of-pocket costs other than fees paid to purchase credit monitoring, which will be addressed separately below.

A number of courts have held that to base standing on past actual harm, plaintiffs in a data breach case must allege not only that their personal data was misused, but also that they suffered economic loss as a result. *See, e.g.*, *Whalen v. Michael Stores Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) ("Whalen does not allege a particularized and concrete injury suffered from the attempted fraudulent purchases . . . ; she never was either asked to pay, nor did pay, any fraudulent charge."); *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1284–85 (N.D. Ala. 2014) (plaintiff alleged unauthorized charges on his debit card but had no standing because he did not allege that he had to pay the charges); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013) ("[Plaintiff] has not pled that actual injury resulted and that she suffered any monetary loss due to the fraudulent charge. . . . In order to have suffered an actual injury, she must have had an unreimbursed charge on her credit card."); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-cv-6060, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (no Article III injury where plaintiff was not financially responsible for unauthorized credit card charge).

Other courts, including some in this district, have held that allegations that plaintiffs' data was misused state an injury in fact, even in the absence of any allegation that they suffered financial consequences as a result. *See In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014) ("*SAIC*") (holding that the "handful" of the plaintiffs who claimed to have suffered actual identity theft "clearly suffered an injury" but ultimately holding they did not have standing because they failed to allege causation); *Welborn v. IRS*, 218 F. Supp. 3d 64, 76–77 (D.D.C. 2016) (holding that plaintiffs who alleged actual identity theft in the form

of false tax returns filed in their names pled injury in fact); *In re Zappos.com, Inc.*, MDL No. 2357, 2016 WL 2637810, at *3–*4 (D. Nev. May 6, 2016).

There is no controlling authority on whether plaintiffs alleging actual harm must allege economic losses from a data breach to show injury in fact. The D.C. Circuit's recent opinion in *Attias v. CareFirst* dealt with allegations of future harm only, and did not directly address the question. 865 F.3d at 626. The Court finds the *Michael Stores* line of cases to be persuasive, and it is inclined to agree that a plaintiff must allege unreimbursed out-of-pocket expenses from the alleged identity thefts to state an injury in fact. *See Michael Stores Inc.*, 689 F. App'x 89 (2d Cir. 2017); *Burton*, 47 F. Supp. 3d at 1280–81; *In re Barnes & Noble*, 2013 WL 4759588, at *3–*4; *Hammond*, 2010 WL 2643307, at *8. However, since the D.C. Circuit has recently stated that a substantial *threat* of identity theft can satisfy the "actual or imminent" prong of the injury-in-fact element, and that identity theft would constitute a concrete and particularized injury, *Attias*, 865 F.3d at 627–29, and it did not mention any need for an out-of-pocket loss, it appears that the Court of Appeals may well ultimately agree with those district judges who have ruled that identity theft is an actual injury, notwithstanding a lack of economic harm. So while this Court finds that only two of the plaintiffs have alleged any injury in fact, it will also go on, as the *SAIC* court did, to consider whether any of the plaintiffs who have experienced credit or IRS irregularities have satisfied the remaining elements of the *Lujan* test and can overcome defendants' other arguments that jurisdiction is lacking.

c. Future Identity Theft and Other Future Harms

The CAC alleges generally that the defendants' actions "placed millions of government workers at a heightened risk of identity theft." CAC ¶ 210; *see also* NTEU Compl. ¶ 92. The CAC plaintiffs allege that as a group, they face an increased risk of experiencing a host of injuries, including: "money and time expended to prevent, detect, contest, and repair identity theft [and]

fraud;" "money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;" and "lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches." CAC ¶ 163.

Numerous individual plaintiffs predicate injury in fact on the likelihood of possible harm in the future. For example:

- Plaintiff Myrna Brown provided sensitive information in an SF 86 form in connection with her employment with the Commerce Department, and she has received notice from OPM that her data was compromised. "Her exposure to the Data Breaches has caused Brown to review her financial accounts with greater frequency. Brown now also reviews her credit reports with greater frequency. Additionally, Brown suffers stress resulting from fear that the theft of her sensitive personal information will impair her ability to obtain future federal employment or security clearances, and fear for the safety of her family members who serve in the military. CAC ¶ 18.

- Plaintiff Maryann Hibbs "works as a Registered Nurse at the Veterans Health Administration, where she has been employed for approximately 23 years." Hibbs also previously served in the Army National Guard. Hibbs provided sensitive information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Hibbs suffers stress resulting from concerns for her personal safety and that of her family members." CAC ¶ 35.

- Plaintiff Robert Slater, who currently serves in the Army, "suffers stress resulting from concerns that the theft of his sensitive personal information will impair his ability to obtain a higher security clearance, or future employment with a government contractor when he leaves the Army. His exposure to the Data Breaches has also caused Slater to review his financial accounts and credit reports with greater frequency to detect fraudulent activity. CAC ¶ 46.

Some plaintiffs claim to be suffering from stress now due to a fear of identity theft, physical harm, or some unspecified threat to their safety in the future, CAC ¶¶ 18–19, 22–25, 28, 30–31, 35, 37, 43–44, 46, 50; NTEU Compl. ¶ 94; and others point to expenses they incurred to

prevent or monitor future identity theft. CAC ¶¶ 17, 21, 25, 28, 34, 40, 41.[15] The Court holds that none of these allegations sets forth an injury in fact.

Future harm is neither concrete nor imminent for standing purposes unless it is "certainly impending," *Pub. Citizen, Inc.*, 489 F.3d at 1293, or it presents a "substantial risk." *Clapper*, 568 U.S. at 414, 422 & n.5. A harm that is "remote, speculative, conjectural, or hypothetical" will not suffice. *Pub. Citizen, Inc.*, 489 F.3d at 1293; *see also Clapper*, 568 U.S. at 422 ("[R]espondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending . . . ."); *Williams v. Lew*, 77 F. Supp. 3d 129, 132–33 (D.D.C. 2015) (plaintiffs' fears, which "rest[ed] on [a] hypothetical premise," did not provide standing because they were based on possible future injury, not a certainly impending one), *aff'd*, 819 F.3d 466, 474 (D.C. Cir. 2016) (holding that a court "cannot exercise jurisdiction based on 'worr[ies] and concern[s]' that lack a reasoned basis") (alterations in original).

The D.C. Circuit recently weighed in on this issue in *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017). Although plaintiffs take the position that the decision binds this Court to find that they have standing to pursue their action, *see* Class Pls.' Suppl. Submission, the Court is not persuaded that the holding covers this case. The Court of Appeals found in that data breach lawsuit that the plaintiffs' plausible allegation that they were subject to a substantial risk of identity theft was sufficient to satisfy the injury-in-fact element of the *Lujan* test, but it drew that conclusion, and found the allegation to be plausible, under circumstances that do not pertain here.

15 For some plaintiffs, the CAC describes a greater degree of attention paid to financial matters, but the allegations do not even go so far as to include the vague references to "stress" or increased concern. For example, with respect to plaintiff Ryan Bonner, the CAC alleges only that Bonner provided sensitive personal information and received notice that the information had been compromised, and that "his exposure to the Data Breaches has caused Bonner to review his credit reports and financial accounts with greater frequency." CAC ¶ 15; *see also* CAC ¶ 13–14, 16–17, 20–21, 26–27, 29, 32–34, 36, 38–42, 45, 47–49.

The *Attias* case arose out of a cyberattack on CareFirst, a health insurance company. After the data breach was reported, plaintiffs sued and predicated standing on an allegation that the breach had exposed them to a heightened risk of identity theft in the future. The district court concluded that the plaintiffs' theory of injury was "too speculative" to satisfy the requirement in *Clapper* that the harm be "clearly impending," and it dismissed the case for lack of subject matter jurisdiction. *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 200 (D.D.C. 2016).

The Circuit Court reversed, stating that the Supreme Court had "clarified that a plaintiff can establish standing by satisfying *either* the 'certainly impending' test *or* the 'substantial risk' test," *Attias*, 865 F.3d at 626–27 (emphasis in original), citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (an allegation of future injury may suffice if the "threatened injury is certainly impending" or there "is a substantial risk that the harm will occur"). It then zeroed in on the latter:

> Under our precedent, "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case, would be identity theft, "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 627, quoting *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 915 (D.C. Cir. 2015). The Court explained that since "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury," the critical question for injury-in-fact purposes "is whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach." *Id.* (emphasis in original). In other words, if plaintiffs can allege that the risk of future harm is substantial, that satisfies the *Lujan* requirement that the injury be imminent.

The Court then combed through the complaint to identify the allegations that made the claim of an increased risk plausible, *id.* at 627–28, and it noted that the complaint alleged that

CareFirst collected and stored sensitive information including credit card and social security numbers.[16] *Id.* It then concluded that the risk was more substantial than the risk presented in *Clapper*. *Id.* at 629.[17] The Court observed that the feared harm in *Clapper* "could only occur through the happening of a series of contingent events, none of which was alleged to have occurred by the time of the lawsuit." *Id.* at 628, citing *Clapper*, 568 U.S. at 410–14. But it found that the CareFirst data breach presented a different situation:

> Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative – at the very least, it is plausible – to infer that this party has both the intent and the ability to use that data for ill. As the Seventh Circuit asked, in another data breach case where the court found standing, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

Id. at 628–29, citing *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015). Based on that analysis, the Court of Appeals found:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.

Attias, 865 F.3d at 629.

While the Court used broad language to announce its conclusion, its determination that the *Attias* allegations were sufficient cannot be separated from its repetition of the rhetorical question

---

16 The district court had based its ruling on the fact that the complaint did not expressly allege that social security or credit card numbers had been *stolen*, and it took into consideration the affidavit of the CareFirst IT Security Official who averred that the most sensitive data, such as social security and credit card numbers, was not included in the data breach. *Attias*, 199 F. Supp. 3d at 196 n.1, 198 n.3, 200–01.

17 The Court of Appeals also noted that the complaint alleged that the theft of the insureds' names, in combination with their birth dates and other subscriber information, created a risk of "medical identity theft" in which an imposter could obtain medical services in their names. *Attias*, 865 F.3d at 628.

posed in *Remijas* and the Seventh Circuit's answer. In other words, standing in *Attias* was predicated on the slender thread that one could fairly assume what the thieves meant to do with the stolen information. While drawing such an inference may have been logical in the case of a domestic crime directed at credit and financial information maintained by a retail establishment or a private health insurer, it is not necessarily logical here, and *Attias* supplies no other principle to follow.

Plaintiffs suggest that this case is "on all fours with the allegations in *Attias*," Class Pls.' Suppl. Submission at 3, but they fail to address the fact that *Attias*, and the case upon which it relies, *Remijas*, were predicated on the theft of credit card information, which the courts inferred could be utilized by the hackers themselves to perpetrate financial fraud. *Remijas*, 794 F.3d at 692–93; *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x. 384, 388 (6th Cir. 2016) (court drew reasonable inference that the domestic criminal theft of personal information from an insurance company was for the fraudulent purposes alleged in the complaint). Moreover, in *Remijas*, there was clear evidence that a large number of the particular credit card numbers that had been stolen had already actually been used. *Id.* at 690. As the district court in *Attias* pointed out:

> *Remijas* involved a data breach of Neiman Marcus's computer systems, which compromised customers' credit card information, social security numbers, and birth dates. Of the 350,000 credit cards whose information was potentially exposed, 9,200 "were known to have been used fraudulently." In other words, the hackers had clearly demonstrated that they had the means and the will either to abuse the information they accessed or to sell it to others who did so.

193 F. Supp. 3d at 200, quoting *Remijas*, 794 F.3d at 690 (citations omitted).

But those allegations are absent here, and the complaint does not allege anything that even comes close.

Plaintiffs have not plausibly alleged that the means to commit credit card or bank fraud were included in this breach, since there is no allegation that those account numbers are called for in the standard forms at issue or that they are provided in the course of background investigations. The CAC alleges in paragraph 144 that the personal information provided to OPM includes "information about financial accounts" and "financial and investment records," *see also* CAC ¶¶ 66, 146, and it states that job applications "include financial information." CAC ¶ 144. But no plaintiff who alleges that he or she suffered from financial fraud, such as the unauthorized use of a credit or debit card, alleges that the card numbers or accounts that were compromised had been supplied to OPM in a government form.

Moreover, a detailed review of the forms themselves, which are specifically referenced in the complaint, *see, e.g.*, CAC ¶¶ 66–70, reveals that they do not ask for account-identifying information. The SF 85, the standard Questionnaire for Non-Sensitive Positions, asks no questions whatsoever concerning finances beyond calling for the identification of present and former employers. *See* https://www.opm.gov/forms/pdf_fill/sf85.pdf.

The more detailed SF 86, the Questionnaire for National Security Positions, does not ask applicants for their active credit or debit card numbers. The form, which is 127-pages long, finally gets to the questions related to business dealings and personal finances on page 63. *See* https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf. And of the many questions asked, only

two call for account numbers of any sort,[18] and those ask about judgments against the applicant for delinquencies, or loans or credit accounts that resulted in foreclosures or cancellations for default – in other words, account numbers that are particularly unlikely to be useful for the perpetration of credit card fraud. But there is no allegation in the complaint that any of the plaintiffs who experienced an unauthorized use of a credit or debit card had provided those particular numbers on the SF 86 or that those were the accounts that were misused.

It has been noted that criminals may use stolen personal information as a step in the process of creating false accounts or engaging in identity theft. *See SAIC*, 45 F. Supp. 3d at 32 ("a criminal could obtain some of a victim's personal information from a data breach and then go 'phishing' to get the rest"). But plaintiffs do not allege that this was the purpose of the cyberattacks, the facts do not suggest that it was, and this would be the classic example of the sort of chain of events

18 The SF 86 asks applicants to provide the following types of financial information:

Page 63: Foreign investments: type of investment, value, date acquired and sold
Page 73: Foreign business activities
Page 100: Whether alcohol or drug use has had a negative impact on finances
Page 106: Any filing for bankruptcy
Page 107: Financial problems due to gambling losses; any failure to pay taxes
Page 108: Whether the applicant has ever been subjected to discipline or required to undergo counseling for misuse of an employer's credit card, and whether he or she is currently using credit counseling services
Page 109: A question on this page asks if the applicant is delinquent in child support payments, or if there has been a judgment entered against him, including any obligations as a sole debtor, tax liens, or delinquencies on other debts, and in that situation, it directs the applicant filling out the form to identify the loan or account number involved.
Page 110: Similarly, a question on page 110 asks about any repossessions, loan foreclosures, loan defaults, debts sent to a collection agency, credit cards cancelled for default, or cards for which the applicant is more than 120 days delinquent, and those numbers are called for as well.

There are no additional questions in the form that seek financial information.

undertaken by a series of independent actors that is inconsistent with the imminence needed for standing.[19]

Also, while this ruling is not based on the original complaints that were consolidated and amended in this multidistrict litigation, the Court notes that many of the plaintiffs specifically alleged that the breaches were widely reported to have been perpetrated by the Chinese government.[20] This was also the conclusion set forth in the U.S. House of Representatives

19 This is why plaintiffs' reliance on *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524 (D. Md. 2016) is misplaced. Plaintiffs argued in their opposition that "put[ting] forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud" can satisfy the clearly impending or substantial risk standard. CAC Pls.' Opp. at 17, quoting *Khan*, 188 F. Supp. 3d at 532. But even if the *Khan* formulation controlled in this district, plaintiffs make neither showing here.

The complaints do not suggest that "the fruits of the data breach" were used for the alleged identity thefts because, as noted above, they do not allege that OPM or KeyPoint maintained the account numbers that were used improperly, nor do they allege that the government forms compromised in the breaches call for that information. The CAC states conclusorily that "[s]tolen federal job applications and investigation forms contain . . . financial records that include bank account and credit card information," CAC ¶ 146, but that allegation is belied by the forms themselves, and no individual plaintiff alleges that he or she provided a credit card, debit card, or bank account number. One individual NTEU plaintiff alleged that through the SF 85P and 86 "he disclosed or authorized the release to OPM of, among other information . . . financial information (including his investment accounts)," NTEU Compl. ¶ 6; another simply alleges that "financial information" was provided, NTEU Compl. ¶ 8; and the third individual plaintiff does not mention finances at all. NTEU Compl. ¶ 7. And both complaints are devoid of allegations that would provide "a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud." *Khan*, 188 F. Supp. 3d at 532.

20 *See, e.g.*, *Am. Fed'n of Gov't Emps. v. OPM*, Case No. 15-1015, Compl. [Dkt. # 1] ¶ 68; *Krippendorf v. OPM*, Case No. 15-1321, Compl. [Dkt. # 1] ¶¶ 61, 73; *Robbeloth v. OPM*, Case No. 15-1449, Compl. [Dkt. # 1] ¶¶ 63, 75; *Brown v. OPM*, Case No. 15-1564, Compl. [Dkt. # 1] ¶ 67; *Bonner v. OPM*, Case No. 15-1617, Compl. [Dkt. # 1] ¶¶ 3 n.4, 54 n.30 (citing press articles); *Waid v. OPM*, Case No. 15-1653, Compl. [Dkt. # 1] ¶¶ 63, 76; *Woo v. OPM*, Case No. 15-1752, Compl. [Dkt. # 1] ¶ 63; *Cavis v. OPM*, Case No. 15-1810, Compl. [Dkt. # 1] ¶¶ 63, 76; *Smith v. OPM*, Case No. 15-1835, Compl. [Dkt. # 1] ¶ 71; *Hobbs v. OPM*, Case No. 15-1927, Compl. [Dkt. # 1] ¶ 63; *Hanagan v. OPM*, Case No. 15-1933, Compl. [Dkt. # 1] ¶ 57; *Fleishell v. OPM*, Case No. 15-2089, Compl. [Dkt. # 1] ¶¶ 7, 81; *Golden v. OPM*, Case No. 16-1253, Compl. [Dkt. # 1] ¶ 80.

Committee on Oversight and Government Reform transmitting the result of a formal investigation into the OPM breach. *See* The OPM Data Breach: How the Gov't Jeopardized Our Nat'l Sec. for More than a Generation, Comm. on Oversight and Gov't Reform, U.S. House of Reps., 114th Congress, Sept. 7, 2016 ("Congressional Report"), at iii, vi, 157. And, while the administration may have been officially circumspect at the time, possibly in light of the classified nature of the information, the state-sponsored nature of the attack was discussed publicly by some individual knowledgeable federal officials. *See* Paul Coyer, *U.S. Gov't Data Breach Exemplifies China's Cyber Insecurities*, Forbes Mag., Jul. 19, 2015 ("The Obama White House has been careful to not formally name China as the perpetrator, yet private security firms which have long experience tracking Chinese cyber activities, Members of Congress who have been briefed by intelligence officials, and even James Clapper, the Director of National Intelligence, have all pointed to China as the likely source of the hacking."); Ellen Nakashima, *Chinese government has arrested hackers it says breached OPM database*, Wash. Post, Dec. 2, 2015. Also, it does not appear that the theory has been revised or abandoned since that time. *See* Devlin Barrett, *Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack*, Wash. Post, Aug. 24, 2017. While a finding concerning the source of the breach is beyond the scope of this proceeding at this juncture, these

circumstances render the Court unable to rely upon the presumption that animated the *Attias* and *Remijas* decisions.[21]

So here, we do have a situation where a "long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm," *Attias*, 865 F.3d at 629, and what is more, the nature of that harm is entirely undefined.

There is no question that plaintiffs have plausibly alleged that the building blocks of some forms of identity theft – social security numbers coupled with names, birthdates, and addresses – were included in the cache of information that was taken from OPM. But the Consolidated Amended Complaint does not point to any particular objective behind the breach beyond the claim that it was carried out to obtain sensitive data for an unspecified "improper use." CAC ¶¶ 7, 117, 128, 132. Neither complaint directly alleges, or marshals any facts that would support an inference, that those behind this attack are likely to use the information for credit card fraud or

---

21 These circumstances further differentiate this case from *Khan*, 188 F. Supp. 3d at 532. The hackers' goal has not been revealed, and there are no allegations that financial fraud or identity theft were the purpose behind the cyberattack.

Plaintiffs contend that they have shown injury in fact anyway because they allege that the breaches were "a targeted and malicious attack," and not an inadvertent part of an ordinary burglary such as the theft of the laptop in the *SAIC* case. CAC Pls.' Opp. at 17–18, citing *Pisciotta v. Old Nat. Bankcorp*, 499 F.3d 629, 632 (7th Cir. 2007); *Am. Fed'n Gov't Emps. v. Hawley*, 543 F. Supp. 2d 44, 45, 50–51 (D.D.C. 2008). But these non-binding cases were decided before *Clapper*, and the standing decisions did not turn whether the data theft was targeted or malicious, rather than inadvertent.

In *Pisciotta*, the Seventh Circuit did not rely on the nature of the hack when ruling that plaintiffs had standing; it simply disagreed with the line of cases requiring plaintiffs whose data has been compromised to experience a misuse of the data in order to state an injury in fact. 499 F.3d at 634. Similarly, the standing decision in *Hawley* did not turn on the nature of the theft of personal data. 543 F. Supp. 2d at 50. More importantly, these cases predate *Clapper*, which made clear that "[a]llegations of *possible* future injury are not sufficient." 568 U.S. at 409, quoting *Whitemore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis added) (internal alterations and quotation marks omitted). In other words, the allegation that the breaches of OPM and KeyPoint were "targeted and malicious" does not eliminate the requirement that plaintiffs' potential harm be certainly impending or, at least, that the risk of harm be "substantial."

identify theft purposes, that they are likely to make it available to other criminals for that purpose, or that the breach has enabled other bad actors to have greater access to the information than they did before. The Court is not suggesting that the breach was insignificant, or that it did not or could not have a serious impact on national security, possibly in ways that could affect or compromise some of the individuals involved. *See* Congressional Report at vi. But there is little alleged to indicate that there is any risk of the particular harm being proposed as a basis for Article III standing – future identity theft – much less, that the risk is now "substantial" in the wake of the events at OPM.[22] The *Attias* Court based its decision on a particular cybercrime in a commercial setting – "the hack and the nature of the data that the plaintiffs allege was taken" – and it did not purport to address every data breach, including those that might be state-sponsored. Since the Court lacks the basis available in *Remijas* or *Attias* to "presume" that the purpose of *this* hack was to facilitate fraud or identity theft,[23] this case is more analogous to *Clapper*, and it is not plausible

22 Plaintiffs' allegations that they face some sort of increased risk are highly conclusory, *see* NTEU Compl. ¶ 92 ("The Defendant's reckless indifference to her obligations has put NTEU members, including Plaintiffs . . . and their families, friends, and other associates at substantial risk of identity theft, thereby subjecting them to financial peril and inconvenience."); and the CAC does not even allege that the threat is substantial. *See* CAC ¶ 7 (plaintiffs' information "remains subject to a continuing risk of additional exposure or theft as a consequence of OPM's ongoing failure to secure it"); CAC ¶ 163 ("As a result of Defendants' violations of law, Plaintiffs and Class members . . . have experienced and/or face an increased risk of experiencing . . . money and time expended to prevent, detect, contest, and repair identity theft, fraud and other unauthorized uses of [government investigation information]; . . . money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns; . . . lost opportunity costs and loss of productivity . . . ."); CAC ¶ 210 ("Defendants' failure to protect the [government investigation information] of Plaintiffs and Class Members abridged their privacy rights . . . and placed millions of government workers at a heightened risk of identity theft, fraud, and other detrimental consequences.").

23 While the Court is bound to accept the factual allegations in the consolidated amended complaint as true, and to resolve any inferences in plaintiffs' favor, it is not required to draw inferences or "presume" circumstances that are not supported by the available public record – which was cited heavily in plaintiffs' own previous allegations – on the matter.

to infer that plaintiffs now face a substantial risk of identity theft based on the allegations in the complaint.

As for the plaintiffs who allege a risk of future bodily injury or express concerns for their personal safety, CAC ¶¶ 13, 18, 22–26, 35, 37, 43, 44, the complaint is devoid of allegations that would give rise to a plausible conclusion that the threat is clearly impending or that the risk became significant as a result of the breach.[24]

With respect to plaintiffs' purchases of credit monitoring and other services to avoid future identity theft, those expenditures also do not constitute an injury in fact either. CAC Pls.' Opp. at 15 (arguing that plaintiffs "reasonably paid to protect themselves" from future injury). It is well-established that incurring "certain costs as a reasonable reaction to a risk of harm" does not provide for injury if "the harm [plaintiffs] seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 402; *Attias*, 865 F.3d at 629 ("To be sure, such self-imposed risk-mitigation costs, when 'incurred in response to a speculative threat,' do not fulfill the injury-in-fact requirement."), quoting *Clapper*, 568 U.S. at 416–17. Even an "objectively reasonable likelihood" of harm sufficient to engender some

24 Plaintiff Jane Doe II bases her injury on the fact that her spouse, an Assistant United States Attorney, submitted sensitive personal information that was compromised. She states that she "experiences significant stress from fear that the exposure of her and her family members' sensitive personal information will cause them to be targeted for retaliatory attacks and bodily harm." CAC ¶ 23. However, Jane Doe II also specifically alleges that her spouse is "responsible for prosecuting large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families," and that he "has received multiple death threats throughout his career and was the subject of an assassination attempt." *Id*. While one cannot deny or minimize the dangers faced by many prosecutors, the complaint makes it clear that the risk arose from the nature of the lawyer's public position, and there is nothing stated that would give rise to an inference that the cyberattack has made the attorney substantially more vulnerable to those who would do him harm.

anxiety does not create standing. *SAIC*, 45 F. Supp. 3d at 26, citing *Clapper*, 568 U.S. at 415–16. Since the risk of identity theft was neither clearly impending nor substantial, plaintiffs' purchases of credit monitoring services do not constitute injury in fact because the risk they sought to prevent is too speculative.

In sum, the Court holds that only the two plaintiffs who alleged that they incurred expenses to rectify the actual fraud or identity theft they experienced, CAC ¶¶ 22, 41, have alleged injury in fact.

2. Causation

This does not end the standing analysis. Those plaintiffs, as well as any other plaintiffs who experienced some sort of identity theft event without an economic loss, lack standing because their alleged injuries are not "fairly traceable" to defendants' challenged actions. *Lujan*, 504 U.S. at 560. Plaintiffs maintain that all they need to allege to show causation is that defendants failed to secure their personal information, hackers stole it, and plaintiffs "consequently were subjected to actual and imminent harm." CAC Pls.' Opp. at 23 ("Nothing further is required at this point to show that the harm is plausibly traceable to Defendants' misconduct."). But the allegations in the complaint do not even rise to the level of "consequently" – plaintiffs repeatedly allege that the breach occurred and an unauthorized use of personal information occurred "thereafter." And while the short discussion of causation at the conclusion of the *Attias* decision may lend some support to plaintiffs' legal position, *see Attias*, 865 F.3d at 629, the Court finds that neither complaint plausibly alleges any connection between the OPM breaches and the claimed harm.

Plaintiffs allege that OPM's failures enabled unknown third parties not before the Court to access their personal information, and they also allege that in some instances, plaintiffs' personal information has been used improperly by unknown parties. As the district court pointed out in *Food & Water Watch v. EPA*:

> The Supreme Court has stated that "[w]hen the suit is one challenging the legality of government action or inaction . . . [and] a plaintiff's asserted injury arises from the government's allegedly unlawful regulation of someone else . . . it becomes the burden of the plaintiff to adduce facts showing that those choices have been or will be made in such a manner as to produce causation and permit redressability of injury."

5 F. Supp. 3d 62, 76 (D.D.C. 2013), quoting *Lujan* at 560–61; *see also Lujan*, 504 U.S. at 562 ("[W]hen the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult to establish.'"), quoting *Allen*, 468 U.S. at 758; *Warth*, 422 U.S. at 505 (holding that plaintiffs must show that, absent the government's allegedly unlawful actions, "there is a substantial probability that they would [not be injured] and that, if the court affords the relief requested, the [injury] will be removed"). Applying these principles in the data breach context, courts in this district have held: "to demonstrate causation, plaintiffs must put forward facts showing that their injuries can be traced to the specific data incident of which they complain and not to any previous theft or data loss incident." *Welborn*, 218 F. Supp. 3d at 79. Plaintiffs do not satisfy this standard for either defendant.

It is true that in the *Attias* case, the D.C. Circuit concluded, "[b]ecause we assume, for purposes of the standing analysis, that plaintiffs will prevail on the merits of their claim that CareFirst failed to properly secure their data and thereby subjected them to a substantial risk of identity theft, we have little difficulty concluding that their injury in fact is fairly traceable to CareFirst." *Attias*, 865 F.3d at 629 (citation omitted). But the Court noted that the issue had not been briefed extensively, *id.*, and there are too many missing links in the chain for that statement to pertain here. As noted above, unlike in *Attias*, plaintiffs do not allege here that either defendant maintained the financial account information used in the alleged identity thefts. Furthermore, they do not allege any facts that plausibly connect the various isolated incidents of the misuse or

attempted misuse of plaintiffs' information to the breaches at issue here. *Cf. Remijas*, 794 F.3d at 692–95 (plaintiffs had standing in a data breach case involving the theft of department store credit card numbers when the stolen card numbers were used after the hack to make fraudulent charges).

"Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012). But allegations of time and sequence are all that plaintiffs provide here: they allege that the breaches occurred and that plaintiffs then learned of the identity theft. *See* CAC ¶ 16 ("Bos . . . received notice from OPM . . . . Bos thereafter learned that an unauthorized credit card account had been opened in his name."); CAC ¶ 30 (plaintiff provided personal information to the federal government, learned of the data breaches, and was "thereafter" informed of unauthorized charges on his debit card); [25] CAC ¶ 14 (plaintiff provided sensitive personal information to the federal government, learned his information has been compromised in the data breaches, and later learned of a false tax return using his and his wife's personal information); *see also* CAC ¶¶ 17, 19, 24, 26, 28–32, 38, 41, 49, 50; NTEU Compl. ¶¶ 66–72, 79–84 (alleging that NTEU plaintiffs submitted "inherently personal information" to OPM, were notified that they were affected by the data breaches announced on June 4 and June 12, 2015, and that plaintiff Gambardella had three fraudulent credit card charges and a fraudulent 2015 tax return filed in his name).[26] The *Attias* Court was able to point to

25 Some allegations do not even include the "thereafter," but simply state that the breach occurred and certain financial irregularities – for which dates are not always provided – also occurred. *See* CAC ¶ 13 ("Plaintiff Travis Arnold . . . received notice from OPM . . . . In May 2015, while reviewing his bank statement, Arnold discovered an unauthorized charge . . . ." And "[w]hile reviewing his credit report, Arnold also learned that between six and ten unauthorized inquiries regarding his credit had been made.").

26 The NTEU complaint does not allege that plaintiffs Howell or Ortino experienced actual identity theft. *See* NTEU Compl. ¶¶ 85–86.

allegations that customers gave CareFirst their credit card information, *Attias*, 865 F.3d at 628, but no plaintiff here has alleged that he provided a credit or debit card number on the SF 85 or SF 86.

Moreover, the events alleged to have occurred after the breach are separated across time and geography, and they follow no discernible pattern: there are a handful of false income tax returns mixed in with such occurrences as a debit card charge here, a charge to a PayPal account (which requires a password) there, several new credit inquiries, the creation of a new cellular phone account, and the cancellation of an account with a local utility. One cannot easily construct any kind of colorable theory that would link these events together, especially given the absence of evidence that the account numbers utilized here were ever provided to OPM. The Court therefore holds that these sets of allegations that two things happened in sequence are not sufficient to show causation.

In addition, to hold defendants accountable for plaintiffs' alleged injuries, the Court would have to presume that the vast majority of identity thefts plaintiffs experienced were not perpetrated by other criminals or were not the result of data breaches of other entities.[27] Such a presumption, with no factual predicate in the complaints besides allegations based on chronology, stretches the notion of traceability in this case beyond constitutional limits, particularly given how common identity theft is in the digital age. *See SAIC*, 45 F. Supp. 3d at 32 ("In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud."). This case is even more attenuated, even if you count all

27 *But see* NTEU Compl. ¶¶ 85–86.

twenty of the CAC plaintiffs alleging some form of fraud: 20 out of 21.5 million is 0.00009 percent.

In the end, plaintiffs can point to nothing that would begin to connect this hack to such random events as an unauthorized spending spree at Best Buy. *See* CAC ¶ 39. Since plaintiffs' allegations of fraudulent financial activity are based on pure speculation about the actions of a chain of unknown third-party wrongdoers who are not before the Court, they are insufficient to establish standing. *See Clapper*, 568 U.S. at 414 (expressing the Court's "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors"). Plaintiffs have not satisfied their burden to adduce facts showing that the choices of third parties "have been or will be made in such manner" to show causation as to OPM or KeyPoint. *Lujan*, 504 U.S. at 562.

For all of these reasons, the Court holds that neither the CAC nor NTEU plaintiffs have Article III standing, and it will grant defendants' motions to dismiss for lack of subject matter jurisdiction pursuant to Rule 12(b)(1).

The Court recognizes, particularly in light of the recent decision in *Attias*, that standing is a very close and difficult question in this case. But there are other significant challenges to subject matter jurisdiction to contend with. Even if plaintiffs have standing, they must establish that there has been a waiver of sovereign immunity that would give the Court authority to hear a claim against the United States, and the bulk of the Privacy Act claims and the APA claim fail for that reason. Furthermore, as a government contractor, KeyPoint also enjoys sovereign immunity, and there is no applicable exception that would allow the lawsuit against the firm to go forward. And in the end, the few CAC plaintiffs who can invoke the Privacy Act fail to state a claim, the CAC

complaint fails to state a claim under the Little Tucker Act, and the NTEU plaintiffs fail to state a constitutional claim.

II. Plaintiffs' Claims Cannot Proceed.

A. Claims Against OPM

1. Plaintiffs' Privacy Act claims must be dismissed.

The CAC plaintiffs' first count against OPM alleges that the agency violated the Privacy Act. CAC ¶¶ 175–85. This act "regulate[s] the collection, maintenance, use, and dissemination of information" by federal agencies, Privacy Act of 1974, § 2(a)(5), 88 Stat. 1896 (codified at 5 U.S.C. § 552a), setting detailed requirements on how agencies should manage their records. 5 U.S.C. § 552a(e). It provides "civil relief to individuals aggrieved by failures on the Government's part to comply with [the Act's] requirements," *Doe v. Chao*, 540 U.S. at 618, when those failures "have an adverse effect on an individual." 5 U.S.C. § 552a(g)(1)(D). Under the Act, the United States is liable for "[a]ctual damages sustained by the individual as a result of" the agency's failure to comply if a court determines that an agency has "acted in a manner which was intentional or willful." 5 U.S.C. § 552a(g)(4)(A) (setting the minimum amount a plaintiff obtains at "no less than $1,000").

Plaintiffs assert that the agency "willfully and intentionally failed to comply with [the Federal Information Security Management Act]" which "adversely affected Plaintiffs and Class members." CAC ¶ 178. In doing so, they contend, OPM violated both the disclosure provision, CAC ¶ 183, and the safeguards provision, CAC ¶ 182, of the Privacy Act.

a. All but two CAC plaintiffs fail to plead actual damages, and therefore the Court lacks subject matter jurisdiction to hear their claims.

The term "actual damages" under the Act is "limited to proven pecuniary or economic harm." *FAA v. Cooper*, 566 U.S 284, 299 (2012); *see also Earle v. Holder*, No. 11-5280, 2012

WL 1450574, at *1 (D.C. Cir. Apr. 20, 2012) (unpublished) ("[B]ecause nothing in appellant's pleadings could be construed as alleging he sustained pecuniary loss as a result of the [defendant's] alleged Privacy Act violation, the district court correctly determined he was not entitled to damages.").

Reading the complaint in the light most favorable to plaintiffs, the Court finds that all but two plaintiffs fail to allege facts that support a plausible inference that they sustained actual damages within the meaning of the Act. Plaintiffs who allege unauthorized charges on their financial accounts do not allege any out-of-pocket or unreimbursed costs resulting from the thefts, *see* CAC ¶¶ 13, 19, 29, 30, 38, 41, 50, so they have not alleged "actual damages" within the meaning of the Act. Further, most plaintiffs alleging other forms of identity theft, such as fraudulent tax returns or the improper use of Social Security numbers, allege that they spent time, but not money, addressing these events. *See* CAC ¶ 13, 14, 16, 17, 21, 24, 26, 28, 29, 31, 32, 39, 45, 49, 50. The plaintiffs who alleged emotional distress arising from the breaches, *see, e.g.*, CAC ¶¶ 22, 41, do not allege "actual damages" under the Act. *Cooper*, 566 U.S at 299, 304. And those plaintiffs who purchased credit monitoring services or incurred other expenses to prevent future identity theft, CAC ¶¶ 17, 21, 25, 28, 34, 40, 41, have not suffered actual damages because expenditures undertaken voluntarily to prevent possible future harm do not constitute actual damages attributable to OPM. *See* 5 U.S.C. § 552a(g)(4); *Welborn,* 518 F. Supp. 3d 82 fn.2 (holding that the plaintiffs' decisions "to spend money on credit monitoring services to prevent potential future harm does not allege actual damages attributable to the [agency]" under the Privacy Act). Therefore, none of these plaintiffs has alleged facts that would support the waiver of sovereign immunity needed to give this Court jurisdiction to hear their claims.

The two plaintiffs who spent money to address actual identity theft did allege "actual damages" under the Act. *See* CAC ¶¶ 22, 41. But their disclosure provision claim fails under Rule 12(b)(6) because it does not plausibly allege that OPM "disclosed" private information as that statutory term has been defined by the D.C. Circuit, and their safeguards provision claim fails because they have not pled sufficient facts to allege that their injuries were "a result of" OPM's actions.

b. The disclosure provision claim fails because OPM did not intentionally or willfully disclose plaintiffs' information within the meaning of the Act.

Plaintiffs allege that OPM violated the disclosure provision of the Privacy Act. CAC ¶ 183. This provision prohibits a federal agency from disclosing "any record . . . contained in a system of records" without the written consent of the "individual to whom the record pertains." 5 U.S.C. § 552a(b). But this claim fails because it hinges on the act of third-party cyber criminals who hacked OPM's systems and were outside of OPM's control. CAC ¶¶ 114–37.

The D.C. Circuit has held, upon review of the Act's "purposes, legislative history, and integrated structure . . . that Congress intended the term 'disclose' to apply in virtually all instances to an agency's unauthorized transmission of a protected record, regardless of the recipient's prior familiarity with it." *Pilon v. U.S. Dep't of Justice*, 73 F.3d 1111, 1124 (D.C. Cir. 1996). In this case, OPM did not "transmit" plaintiffs' information: a third party stole it. *See also VA Data Theft Litig.*, 2007 WL 7621261, at *6 ("It is difficult to imagine how an illegal act of a third party over whom the [agency] had no control could . . . constitute an intentional or willful disclosure by the [agency]"). Accordingly, the Court holds that plaintiffs' allegations do not plead an intentional or willful "disclosure" by OPM.

c. While plaintiffs have alleged a willful violation of the safeguards provision of the Privacy Act, their claim fails because they do not allege sufficient facts to show that their injuries were "a result of" OPM's conduct.

Plaintiffs also contend that OPM violated the safeguards provision of the Act. CAC ¶ 182. This provision requires federal agencies to "establish appropriate administrative, technical, and physical safeguards" to protect agency records. 5 U.S.C. § 552a(e)(10). To be an "intentional or willful" violation of this provision of the Privacy Act, an agency's actions must be "greater than gross negligence." *Waters v. Thornburgh*, 888 F.2d 870, 875 (D.C. Cir. 1989), *abrogated on other grounds by Chao*, 540 U.S. at 618. Its actions must be "so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham v. U.S. Navy*, 813 F.2d 1236, 1242 (D.C. Cir. 1987), quoting *Wisdom v. Dep't of Hous. & Urban Dev*., 713 F.2d 422, 425 (8th Cir. 1983).

Courts have held that allegations that an agency has been warned "of recurring, systemic, and fundamental deficiencies in its information security . . . if proven, would support a finding that defendants were warned of the deficiencies in their information security but failed to establish proper safeguards." *Hawley*, 543 F. Supp. 2d at 52 (holding that allegations that the Office of Inspector General "repeatedly informed" the agency of problems with its information security pled "intentional and willful" conduct); *see also VA Data Theft Litig.*, 2007 WL 7621261, at *4–*5 (allegations that an agency had been "warned repeatedly of deficiencies in [its] information security and yet failed to do anything to establish proper safeguards" were sufficient to plead that the agency "acted with something greater than gross negligence").

Plaintiffs here allege that OPM was warned repeatedly by its Office of Inspector General that the agency's computer security was deficient. CAC ¶¶ 84–113 (alleging that OPM was warned of information security deficiencies, including that it "fail[ed] to implement or enforce multi-factor authentication," "failed to promptly patch or install security updates for its systems,"

"lacked a mature vulnerability scanning program to find and track the status of security weaknesses . . . and failed to continuously monitor the security controls of its software systems," and "failed to engage in appropriate oversight of its contractor-operated systems"). They also allege that its failure to correct these specific deficiencies identified by the Inspector General "enabled hackers to access and loot OPM's systems for nearly a year without being detected," CAC ¶ 134; that "inadequate patching of software systems contributed to the [breaches]," CAC ¶ 135; and that "OPM's failure to implement . . . tiered identity management controls for system administrators exposed hundreds of its sub-networks, instead of a single sub-network, to breach," and if it implemented such controls, "the intrusion would have been detected earlier and the cyber thieves prevented from accessing the entire OPM network." CAC ¶ 137. Assuming the truth of the allegations in the complaint, as required when resolving a motion to dismiss, the Court holds that these factual statements do allege that OPM acted in an "intentional or willful" manner. *See Hawley*, 543 F. Supp. 2d at 52.

But the allegations still fail to state a claim because they plead facts insufficient for the Court to plausibly infer that OPM's failure to comply with the safeguards provision "ha[d] an adverse effect" on plaintiffs, 5 U.S.C. § 552a(g)(1)(D), or that their damages are "as a result of" the agency's failures. 5 U.S.C. § 552a(g)(4)(A). *See, e.g., Lugo v. U.S. Dep't of Justice*, 214 F. Supp. 3d 32, 41 (D.D.C. 2016) (holding that plaintiffs must plead "a 'causal connection' between the agency violation and the adverse effect"), quoting *Doe v. Dep't of Justice*, 660 F. Supp. 3d 31, 49 (D.D.C. 2009).

The two plaintiffs who allege actual damages make only a temporal connection between the OPM breaches and their damages. *See* CAC ¶ 22 (alleging that plaintiff was notified of the breaches, that in August of 2015, the FBI informed her "that her [government investigation

information] had been acquired by the so-called Islamic State of Iraq and al-Sham," and that while reviewing her credit report at an unspecified time, she discovered accounts had been fraudulently opened in her name and she purchased credit repair services and a copy of her credit report); CAC ¶ 41 (alleging that plaintiff was notified of the breaches; in June of 2015, she learned of fraudulent activity related to her account with an electrical utility; "additionally," she learned of fraudulent purchases on her debit card and two credit cards; and she purchased credit monitoring and repair). For the same reasons that plaintiffs do not plead injuries traceable to OPM for standing purposes, these allegations of problems that arose after the breaches are insufficient to plausibly allege that OPM's actions "ha[d] an adverse effect" on them or that that their identify thefts were "a result of" the OPM's actions or the breaches. Plaintiffs do not allege that OPM obtained or stored the account numbers that were improperly used – neither complaint alleges that the government was in possession of anyone's debit card number. And the facts alleged, as well as public statements about the breaches, suggest the attacks were not made for the purpose of ringing up retail charges or defrauding the electric company. Thus, it is equally if not more possible that plaintiffs' damages were the result of other criminal activities unrelated to the OPM breaches, and plaintiffs fail to allege facts, as opposed to conclusions, that would tie them to OPM.

Therefore, the Court will dismiss the few claims under Privacy Act over which it arguably has jurisdiction for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6).

2. Plaintiffs fail to state a claim under the Little Tucker Act.

CAC plaintiffs' second count alleges that OPM violated the Little Tucker Act, 28 U.S.C. § 1346. This act authorizes a "civil action or claim against the United States, not exceeding $10,000 in amount, founded . . . upon any express or implied contract with the United States." *Id.* § 1346(a)(2). But in this case, there is no contract.

Plaintiffs allege in connection with federal employment that, along with all class members who completed SF 85 and SF 86 forms, they were in a contractual relationship with OPM. CAC ¶ 192. The contractual claim is based on the fact that each form contains a statement advising job applicants that the information called for "will be protected from unauthorized disclosure." *See, e.g.*, SF 86 at 2. It also warns that the information "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. § 552a(b)], and by routine uses," and each form lists eleven permitted uses. CAC ¶¶ 68–69; *see, e.g.*, SF 86 at 2. Plaintiffs assert that they relied on their "reasonable expectation and understanding that OPM was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes," and that OPM breached this agreement. CAC ¶¶ 192–93.

The statements in these forms, however, do not create a contract between plaintiffs and OPM because a pre-existing legal duty cannot form the basis for a contract. *Allen v. United States*, 100 F.3d 133, 134 (Fed. Cir. 1996) ("Performance of a pre-existing legal duty is not consideration."), citing Restatement (Second) of Contracts § 73 (1981) ("Performance of a legal duty owed to a promisor which is neither doubtful nor the subject of honest dispute is not consideration[.]"); *Floyd v. United States*, 26 Cl. Ct. 889, 891 (1992) ("That which one is under a legal duty to do, cannot be the basis for a contractual promise."), *aff'd*, 996 F.2d 1237 (Fed. Cir. 1993); *Youngblood v. Vistronix, Inc.*, No. 05-21, 2006 WL 2092636, at *4 (D.D.C. July 27, 2006) ("It is a general maxim of contract law that a party cannot offer as consideration a duty that the party is already obligated to perform.").

Plaintiffs contend that defendants' reference to the Privacy Act obligations in the forms overlooks OPM's separate duty to protect submitting information "from unauthorized disclosure." CAC Pls.' Opp. at 106 (quoting forms and arguing "[t]his promise stands by itself" and "is not

defined by reference to the Privacy Act"). But the single sentence merely acknowledges OPM's obligation to handle the information on the forms in accordance with federal law.

In any event, plaintiffs fail to allege facts to support the plausible inference of a contract. There is no offer because government forms are not considered binding contracts. *See, e.g.*, *Chattler v. United States*, 632 F.3d 1324, 1330 (Fed. Cir. 2011) (holding that a passport applicant's completion of a form for faster processing is a request for such processing, not a promise by the government to do so). Further, there was no acceptance because no one authorized to bind the government entered into a contract with plaintiffs. *Stout Rd. Assocs., Inc. v. United States*, 80 Fed. Cl. 754, 756 (2008) ("Only government officials who possess a Contracting Officer's warrant are authorized to bind the United States to a contract."). And as already explained above, there is no consideration. *Allen*, 100 F.3d at 134; *Floyd*, 26 Cl. Ct. at 891 (language in a contract that is "essentially no more than a restatement of a pre-existing legal duty . . . cannot stand as consideration sufficient to support a return promise").

3. The Court lacks subject matter jurisdiction to hear plaintiffs' claim under the APA.

The third count in the Consolidated Amended Complaint seeks declaratory and injunctive relief under the APA for OPM's alleged violations of the Privacy Act and FISMA. CAC ¶ 198 (alleging that "OPM acted arbitrarily and capriciously, [and] abused its discretion" when it violated the Privacy Act, FISMA, and regulations and technical standards for data security). Plaintiffs allege a series of failures by OPM relating to the operation of its computer and software systems, both before its systems were breached and after. CAC ¶¶ 200, 202.

The APA may serve as the waiver of sovereign immunity for claims brought by an individual who "suffer[ed a] legal wrong because of agency action, or [was] adversely affected or aggrieved by agency action." 5 U.S.C. § 702. It cannot, however, be invoked when another statute

"expressly or impliedly forbids the relief which is sought." *Id.* The Privacy Act limits the injunctive relief available under the statute to an order that an agency correct inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C §§ 552a(g)(1)(A), (2)(A), or give individuals access to their records. *Id.* § 552a(g)(1)(B). No other forms of injunctive relief are available to plaintiffs for violations of the Act. *See Edison v. Dep't of Army*, 672 F.2d 840, 846–47 (11th Cir. 1982), citing *Parks v. IRS*, 618 F.2d 677, 683–84 (10th Cir. 1980); *Cell Assocs., Inc. v. Nat'l Insts. of Health*, 579 F.2d 1155, 1161–62 (9th Cir. 1978); *Houston v. U.S. Dep't of Treasury*, 494 F. Supp. 24, 29 (D.D.C. 1979). Given this, plaintiffs cannot invoke the APA to obtain injunctive relief that the Privacy Act forbids.[28]

Plaintiffs' assertions that OPM's violations of the FIMSA warrant judicial review under the APA are similarly unavailing. The APA provides for judicial review of all "final agency action for which there is no other adequate remedy in a court," 5 U.S.C. § 704, except when "statutes preclude judicial review" or the "agency action is committed to agency discretion by law." *Id.* § 701(a). FISMA requires federal agencies to comply with information "security standards and conduct annual, independent evaluations of their information security." *Trusted Integration, Inc. v. United States*, 679 F. Supp. 2d 70, 74 (D.D.C. 2010), citing 44 U.S.C. §§ 3543–45. Although the D.C. Circuit has not ruled on the issue, it has indicated that the choices an agency makes in carrying out its FISMA obligations are not subject to judicial review. *See Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) ("Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in

28 Counsel for the CAC plaintiffs cited no authority for his contention that "the Court, under the APA, has the power to enforce the obligations of the agency to take the necessary measures to protect . . . private information . . . [I]t's really the claim of last resort when there's no alternative from the perspective of the class members to vindicate those rights." Hr'g Tr. at 31.

carrying out its FISMA obligations."). The Court holds that OPM's actions in carrying out the statute's requirements is committed to the agency's discretion, and not subject to judicial review under the APA. *Welborn*, 218 F. Supp. 3d at 81 ("[E]ach agency head is delegated full discretion in determining how to achieve [FISMA's] goals, which removes it from APA review.").

4. The NTEU plaintiffs fail to state a constitutional claim.

The NTEU plaintiffs have brought just one claim on behalf of themselves and the NTEU members whose personal information was exposed by the breaches: that OPM violated their constitutional right to informational privacy. NTEU Compl. ¶¶ 95–98. The Court holds that the NTEU complaint fails to allege a legally cognizable constitutional claim.

Legal authority on the existence of a constitutional right to informational privacy is limited. The Supreme Court has addressed the matter in only three cases, and in those cases, it assumed – but did not expressly recognize – the existence of such a legal interest. *See NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457–65 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600, 605–06 (1977). Based on the assumption that the Constitution protects an individual's "interest in avoiding disclosure of personal matters," *NASA*, 562 U.S. at 138, quoting *Whalen*, 429 U.S. at 599; *Nixon*, 433 U.S. at 457, the Court has examined whether there are constitutional limits on the amount or type of information the government may collect from citizens in three different contexts.

In *Whalen*, the Supreme Court considered a challenge to a New York statute that required physicians and pharmacists to report prescription information for certain narcotics to the state health department, which would maintain the information in a centralized computer file. 429 U.S. at 593. The plaintiffs expressed a fear that the computerized data would be misused, and they claimed that the statute invaded a constitutionally protected "zone of privacy," which included an "individual interest in avoiding disclosure of personal matters" and an interest in the right to make

important individual decisions independently. *Id.* at 598–600. But the Court found that the New York program did not pose a threat to either interest. *Id.* In a "word about issues we have not decided," the Court observed that the government's right to collect and use private data for public purposes is "typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures," and "that in some circumstances, that duty arguably has its roots in the Constitution." *Id.* at 605. But since it found that the New York statute reflected "a proper concern with, and protection of, the individual's interest in privacy," and that no right or liberty protected by the Constitution had been invaded, the Court pointedly stated: "[w]e therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions." *Id.* at 605–06.

In *Nixon*, the Court rejected a constitutional challenge to the Presidential Recordings and Materials Preservation Act, 44 U.S.C. § 2111, which compelled the President to turn over his Presidential papers and recorded conversations for review, and which the President claimed would violate his constitutional right to privacy. 433 U.S. at 429, 434, 454–55, 459. Emphasizing that the statute "mandate[d] regulations . . . aimed at preventing undue dissemination of private materials," *id.* at 458, the Court concluded that the public interest in preserving the documents outweighed any expectation of privacy the former President may have had in the materials, *id.* at 465, and it rejected his claim without ruling on the question of whether the President had a valid constitutional interest in the first place. *Id.* at 457 ("We *may* agree with appellant that, at least when Government intervention is at stake, public officials, including the President, are not wholly without constitutionally protected privacy rights in matters of personal life unrelated to any acts done by them in their public capacity.") (emphasis added).

Finally, in *NASA*, the Court held that challenged portions of the federal government's standard background investigation did not violate any constitutional right to informational privacy, emphasizing that the Privacy Act "covers all information collected during the background-check process" and imposes obligations for nondisclosure and criminal liability for willful violations of those obligations. 562 U.S. at 148, 156 (noting that in the context of hiring federal employees, the government "has a much freer hand in dealing 'with citizen employees than it does when it brings its sovereign power to bear on citizens at large'") (citation omitted).

Faced with this lack of definitive guidance from the Supreme Court, the D.C. Circuit has simply assumed in cases involving the collection of information that keeping one's information private may have a constitutional dimension, and it has not gone on to resolve the issue. *See, e.g.*, *Franklin v. Dist. of Columbia*, 163 F.3d 625, 638–39 (D.C. Cir. 1998); *Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 795 (D.C. Cir. 1997); *Nat'l Fed'n of Fed. Emps. v. Greenberg*, 983 F.2d 286, 294–95 (D.C. Cir. 1993); *United Steelworkers of Am., AFL-CIO-CLC v. Marshall*, 647 F.2d 1189, 1240–41 (D.C. Cir. 1980). Indeed, the Court expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps.*, 118 F.3d at 791 ("Were we the first to confront the issue we would conclude with little difficulty that such a right does not exist."); *see also Greenberg*, 983 F.2d at 293–94 (expressing the view of two panel members that *Whalen* is ambiguous as to the right's existence).[29] But given the uncertainties surrounding the issue and the absence of any clear indication from the Supreme Court, the D.C. Circuit in the *American Federation* case declined to

29 *But see Am. Fed'n of Gov't Employees*, 118 F.3d at 792 (suggesting in dicta the existence of a constitutional right to privacy in personal information), citing *United States v. Hubbard*, 650 F.2d 293, 304–06 (D.C. Cir. 1980); *Doe v. Webster*, 606 F.2d 1226, 1238 n.49 (D.C. Cir. 1979); *Utz v. Cullinane*, 520 F.2d 467, 482 n.41 (D.C. Cir. 1975).

"enter the fray by concluding that there is no such constitutional right." 118 F.3d at 793. It found reaching the issue to be unnecessary since the governmental interest in obtaining the information were sufficiently weighty to justify the intrusions into agency employees' privacy that were challenged in that case. *Id.*

Given this reticence on the part of the higher courts, and the absence of binding precedent one way or the other, this Court also finds it prudent to avoid wading into the legal waters surrounding the existence or scope of any constitutional right to informational privacy in general when it is not necessary to do so. And it is not necessary here because the NTEU claim is asking the Court to recognize a constitutional violation that no court has even hinted might exist: that the assumed constitutional right to informational privacy would be violated not only when information is disclosed, but when a third party *steals* it. *See* NTEU Compl. ¶¶ 96–98; NTEU's Opp. at 25–44 (arguing that the government has an affirmative duty "grounded in the constitutional right to informational privacy" to safeguard plaintiffs' private data). In other words, even if an individual who completes an SF 85 or SF 86 has a constitutional right to privacy in the information he or she is being asked to provide, it is well-established that the government has the right to gather that information. And even if it might violate the Constitution for the government to then deliberately disclose the information,[30] there is no authority for the proposition that the Constitution gives rise to an affirmative duty – separate and apart from the statutory requirements enacted by Congress – to protect the information in any particular manner from the criminal acts of third parties. *See, e.g.*, *Harris v. McRae,* 448 U.S. 297, 317–318 (1980) (discussing the Due Process Clause of Fifth

30 *See Eagle v. Morgan*, 88 F.3d 620 (8th Cir. 1996); *Sheets v. Salt Lake Cty.*, 45 F.3d 1383 (10th Cir. 1995); *James v. Douglas*, 941 F.2d 1539 (11th Cir. 1991); *Fadjo v. Coon*, 633 F.2d 1172 (5th Cir. 1981).

Amendment and declining to "translate the limitation on governmental power implicit in the Due Process Clause" into an affirmative obligation on the government).

At bottom, what the NTEU plaintiffs allege is a violation of the Privacy Act, *see* NTEU Compl. ¶ 97 ("By failing to heed the repeated warnings of OPM's OIG and otherwise failing to satisfy obligations imposed on her by statute and other appropriate authority, the Defendant has manifested reckless indifference to her obligation to safeguard personal information . . . ."), but they have not brought a Privacy Act claim or alleged the facts that would enable them to do so, and they cannot find support for the allegedly unfulfilled "obligation" in the Constitution.

The sole source plaintiffs identify for the existence of the affirmative duty they would have this Court enforce is a law review article. NTEU's Opp. at 37, citing A. Michael Froomkin, Government Data Breaches, 24 Berkley Tech. L. J. 1019, 1049 (2009) ("When 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."). Given the absence of any binding precedent – or even any persuasive writing from other courts – that recognizes a

constitutionally based duty to safeguard personal information,[31] and the D.C. Circuit's expressed skepticism about the existence of a right to informational privacy in the first place, this Court is compelled to hold that plaintiffs have failed to state a constitutional claim.[32]

B. Claims Against KeyPoint

The CAC plaintiffs assert that KeyPoint is liable for negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, violations of the Fair Credit Reporting Act, and various state statutes governing unfair and deceptive trade practices and data breaches. CAC ¶¶ 216–75. The Court holds that plaintiffs' claims against KeyPoint must be dismissed because the firm is immune from suit as a government contractor.

The Supreme Court has held that "government contractors obtain certain immunity in connection with work which they do pursuant to their contractual undertakings with the United States." *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672 (2016), quoting *Brady v. Roosevelt S.S. Co.*, 317 U.S. 575, 583 (1943). That immunity applies unless a contractor "violates . . . federal law and the Government's explicit instructions" or "ha[s] 'exceeded his authority' or the authority 'was not validly conferred.'" *Id.* at 672–73, quoting *Yearsley v. W.A. Ross. Constr. Co.*, 309 U.S. 18, 20–21 (1940) ("[A]uthority to carry out [a] project [is] validly conferred, that is, [when] what

31 Plaintiffs cite a number of cases from other circuit courts for the proposition that the existence of the constitutional zone of privacy "is firmly established." *See* NTEU's Opp. at 29, n.7, citing *Denius v. Dunlap*, 209 F.3d 944, 955–56 (7th Cir. 2000); *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996); *Sheets v. Salt Lake Cty.*, 45 F.3d 1383, 1388 (10th Cir. 1995); *James v. Douglas*, 941 F.2d 1539, 1544 (11th Cir. 1991); *Woodland v. City of Houston*, 940 F.2d 134, 138 (5th Cir. 1991); *Walls v. Petersburg*, 895 F.2d 188, 192–95 (4th Cir. 1990); *Barry v. City of New York*, 712 F.2d 1554, 1558–64 (2d Cir. 1983); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577–80 (3d Cir. 1980). But those cases do not hold that the constitutional right would be violated when a third party steals private information from the government.

32 Since the Court finds that the NTEU case should be dismissed under both Rule 12(b)(1) and Rule 12(b)(6), it does not reach the issue of sovereign immunity, which was addressed only briefly by the parties.

[is] done was within the constitutional power of Congress, there is no liability on the part of the contractor for executing [Congress's] will.").

There is no dispute that KeyPoint was acting pursuant to a valid contract with OPM. CAC ¶¶ 1, 123 (alleging that KeyPoint was acting pursuant to a contract with the United States at the time of the events underlying the complaint). So the question is whether the complaint plausibly alleges that KeyPoint violated federal law and OPM's explicit instructions or exceeded its authority under the contract. *Campbell-Ewald Co.*, 136 S. Ct. at 672–73, quoting *Brady*, 317 U.S. at 575.

1. KeyPoint has derivative immunity because it was a government contractor.

Plaintiffs argue that because KeyPoint "violated section 552a(e)(10) . . . [and] section 552a(b) of the Privacy Act," it is not protected by derivative government immunity. CAC Pls.' Opp. at 60–61. KeyPoint maintains that this argument does not provide a basis to abrogate its immunity because a contractor cannot violate the Privacy Act. KeyPoint Mem. at 20.

The Privacy Act imposes requirements on each "agency" that maintains a system of records, *see, e.g.*, 5 U.S.C. § 552a(d), and section 552a(a)(1) of the statute refers to 5 U.S.C. § 551, the Freedom of Information Act, for the definition of the term agency:

> "[A]gency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency . . . .

5 U.S.C. § 552(f)(1). With respect to government contractors, the statute expressly provides:

> When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.

5 U.S.C. § 552a(m)(1). Thus, the Act requires that the *agency* ensure that the requirements of the Act are implemented; it does not hold contractors responsible for doing so. *See Metro. Life Ins. Co. v. Blyther*, 964 F. Supp. 2d 61, 71 (D.D.C. 2013), citing *Unt v. Aerospace Corp*., 765 F.2d 1440, 1447 (9th Cir. 1985) (dismissing Privacy Act claims against insurance companies that cover life insurance for federal employees and holding that "the Privacy Act does not apply to government contractors"); *see also Abdelfattah v. DHS*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) ("[t]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individuals"); *see also Martinez v. Bureau of Prisons*, 444 F.3d 620, 624 (D.C. Cir. 2006) (holding that the Act "authoriz[es] suit against an 'agency'" and affirming dismissal of Privacy Act claims against individuals because individuals are not federal agencies).

2. Plaintiffs do not adequately identify a portion of KeyPoint's contract with OPM that KeyPoint breached.

Plaintiffs argue, though, that KeyPoint "breached the terms of its contract with OPM . . . [because] [f]ederal contracts necessarily incorporate the requirements of the Privacy Act" via section 552a(m)(1). CAC Pls.' Opp. at 61–62, citing CAC ¶ 123 ("The contract between OPM and KeyPoint incorporates the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1)").

But this is simply an attempt to do indirectly what plaintiffs cannot do directly, and it fails as well. It is true that section 552a(m)(1) provides: "[w]hen an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system." 5 U.S.C. § 552a(m)(1); *see also* 48 C.F.R. § 24.102(a). But the implementing regulation goes on to provide: "the system of records operated under the contract is deemed to be maintained by the agency," 42 C.F.R. § 24.102(c), and section 552a(m)(1) makes

clear that the contractor and its employees shall be considered employees of the agency. So this provision does not supply a basis to transfer Privacy Act liability to KeyPoint.

Even if one can draw an inference that pursuant to this provision of the Act, OPM imposed contractual requirements that prohibited KeyPoint from "disclosing" any record in accordance with § 552a(b), and bound it to establish appropriate safeguards under § 552a(e)(1), the complaint does not allege facts that would show that these presumed contractual terms were violated. There is no allegation in the complaint that KeyPoint "disclosed" anything – the complaint alleges that KeyPoint was the victim of a breach, and that a set of its log-in credentials was "stolen." CAC ¶¶ 4, 117, 127, 133.

With respect to safeguards, plaintiffs conclusorily allege that KeyPoint breached its contract with OPM because it "fail[ed] to ensure the security and confidentiality of records and to protect against known and anticipated threats," CAC ¶ 123, and by "unreasonably failing to safeguard its security credentials and Plaintiffs' [government investigation information]." CAC ¶ 122. But these general statements do not supply any facts and do not state a claim for breach of contract. Plaintiffs allege that KeyPoint "lack[ed] software logs to track malware entering its systems and data exiting its systems," *id.* ¶ 121, but they can point to no provision of the contract between OPM and KeyPoint requiring those measures. A plaintiff must provide "factual content [in her complaint] that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged," *Brown v. Sessoms*, 774 F.3d 1016, 1020 (D.C. Cir. 2014), quoting *Iqbal*, 556 U.S. at 678, and those facts are lacking here.

Finally, plaintiffs make only conclusory allegations that KeyPoint exceeded its authority in executing its contract with OPM. *See* CAC ¶ 122 (alleging that "[b]y unreasonably failing to safeguard its security credentials and Plaintiffs' and Class members' [government investigation

information], KeyPoint departed from its mandate, exceeded its authority, and breached its contract with OPM"). These allegations offer no more than "labels and conclusions" and so they do not suffice to state a claim. *Iqbal*, 556 U.S. at 678 (2009), quoting *Twombly*, 550 U.S. at 555.

3. Even if KeyPoint acted negligently, it did not lose its sovereign immunity.

Finally, plaintiffs maintain that "derivative sovereign immunity is not available to contractors who act negligently in performing their obligations under the contract." CAC Pls.' Opp. at 62, quoting *In re Fort Totten Metrorail Cases*, 895 F. Supp. 2d 48, 74 (D.D.C. 2012). But *Fort Totten* does not eliminate contractor immunity any time a plaintiff alleges negligence by government contractor.

Applying the doctrine of derivative immunity for government contractors for the first time in this circuit, *Fort Totten* involved a claim against a subcontractor that had agreed to replace certain safety features on train tracks and conduct safety tests of those features. 895 F. Supp. 2d at 72–73. The plaintiffs asserted that the subcontractor "negligently failed to perform safety and compatibility testing in violation of its contractual obligations and applicable standards of care," but the contractor asserted it had derivative sovereign immunity under *Yearsley*. *Id.* at 74–75. The purported sovereign entity, Washington Metropolitan Area Transit Authority ("WMATA"), filed cross-claims against the subcontractor for breach of contract and negligence. *Id.* at 75.

In deciding whether the subcontractor had immunity, the court analyzed the various claims against the subcontractor, considering whether they were predicated on the subcontractor carrying out its contract with WMATA or on the subcontractor's breach of that contract and negligence in performing its obligations under the contract. *Id.* WMATA asserted that the subcontractor was required by the contract to ensure the compatibility of certain products to perform the requisite safety testing but failed to carry out these obligations. *Id.* Thus, the court concluded, "the very premise of these claims is that [the contractor] acted *against* the 'will of the sovereign' by

breaching its contractual duties to [the sovereign entity] and by performing negligently under the contract," undermining the contractor's attempt to invoke derivative immunity. *Id.* The court held that the contractor was "not entitled to derivative sovereign immunity under *Yearsley* as to these claims." *Id.*

The instant case is distinguishable from *Fort Totten*, which involved the unique circumstance where the governmental entity itself was making the allegation. Here, plaintiffs provide only conclusory allegations that KeyPoint exceeded its authority or acted negligently, and its conclusory allegations are based on its contentions that KeyPoint violated FISMA and breached its contract with OPM. *See* CAC ¶¶ 122–24. But as explained above, plaintiffs do not identify any contract provisions that KeyPoint allegedly violated, and their claims that it violated federal law cannot stand. And importantly, the sovereign in this case, OPM, does not disavow the actions of KeyPoint. Indeed, the complaint indicates as much, alleging that "OPM did not terminate or suspend its contract with KeyPoint." CAC ¶ 5. Thus, plaintiffs fail to plead facts sufficient to allege that KeyPoint violated OPM's explicit instructions or exceeded its authority under its contract with the agency.[33]

33 Plaintiffs also cite *Worcester v. HCA Management Co.*, 753 F. Supp. 31 (D. Mass. 1990), to support their argument that KeyPoint does not have derivative sovereign immunity, but that case is inapplicable. *Worcester* holds that, in addition to the exceptions recognized in *Campbell-Ewald*, a separate exception exists "when a private corporation who performs governmental duties pursuant to contractual authority from the government is sued for negligence in the performance of the[] duties." 753 F. Supp. at 38. The court relied on *Brady v. Roosevelt*, which held that a contractor cannot "escape liability for a negligent exercise of . . . delegated power," 317 U.S. at 583, because "the government is not the 'real party in interest'" when the contractor acts negligently. *Worcester*, 753 F. Supp. at 38, quoting *Brady*, 317 U.S. at 584. But *Brady* concerned "whether respondent can escape liability for a negligent exercise of . . . delegated power if we assume that by contract it will be exonerated or indemnified [by the federal government]." *Brady*, 317 U.S. at 583–84. Since KeyPoint will not be indemnified by the federal government in this case, *Brady* is not directly applicable, and *Worcester* is not binding on this Court in any event.

Accordingly, all of plaintiffs' claims against KeyPoint will be dismissed for lack of subject matter jurisdiction.

C. Claims against both defendants for declaratory judgment and injunctive relief will be dismissed for lack of subject matter jurisdiction.

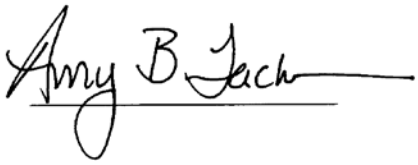
Finally, the Court will dismiss the CAC plaintiffs' Count IV, which seeks a declaration that defendants' conduct is unlawful, a judgment requiring them to indemnify plaintiffs for their economic injury and provide "free lifetime identity theft protection services," and an order that OPM implement a data security plan that complies with the Privacy Act and FISMA. CAC ¶¶ 208–15. They assert that equitable relief is warranted under the APA, the Declaratory Judgment Act, the common laws and statutory provisions that KeyPoint violated, and the Court's inherent authority. CAC ¶ 209.[34] But, as explained above, the APA does not provide relief for plaintiffs' claims. Also, as explained above, neither the Privacy Act, the Little Tucker Act, nor the APA provide plaintiffs the relief they seek, and the United States may not be sued without a waiver of sovereign immunity. *United States v. Mitchell*, 463 U.S. 206, 212 (1983). Finally, the Declaratory Judgment Act does not provide a private right of action or an independent source of federal jurisdiction, *see*, *e.g.*, *Ali v. Rumsfeld*, 649 F.3d 762, 778 (D.C. Cir. 2011). Accordingly, the Court also dismisses Count IV of the CAC.

CONCLUSION

For the reasons set forth above, the Court will dismiss plaintiffs' Consolidated Amended Complaint and the NTEU Complaint for lack of subject matter jurisdiction based on both standing and sovereign immunity grounds, and the Court also finds that the CAC fails to state a claim under

34 Characterizing their request for relief for indemnity from economic harm as seeking "equitable relief" does not allow plaintiffs to circumvent the Privacy Act's requirement that they suffer actual damages to obtain relief under the Act, *Cooper*, 132 S. Ct. at 1453, nor does it allow plaintiffs to circumvent the APA's prohibition against monetary damages. 5 U.S.C. § 702 (providing for judicial review of claims "seeking relief other than money damages").

the Privacy Act and the Little Tucker Act, and that the NTEU complaint fails to state a constitutional claim. A separate order will issue.



AMY BERMAN JACKSON
United States District Judge

DATE: September 19, 2017