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	

PLAINTIFFS' CONSOLIDATED OPPOSITION TO
DEFENDANTS' MOTIONS TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Statutes

Other Authorities

INTRODUCTION

Plaintiffs' complaint details the security failures of the U.S. Office of Personnel Management ("OPM") and KeyPoint Government Solutions, Inc. ("KeyPoint") that led to the 2013 and 2014 data breaches ("Data Breaches"). Plaintiffs have standing to sue because Defendants' actions and inactions resulted in a range of concrete and imminent injuries. These injuries have occurred and there is a substantial risk they will occur in the future. Plaintiffs incurred damage attributable to identity theft, fraud, risk mitigation, and emotional distress. All class members share an interest in injunctive relief at both an individual and institutional level to ensure their protection from future harm, including from further misuse of the highly sensitive information they entrusted to Defendants. Plaintiffs' injuries are redressable and causally connected to Defendants' conduct, as they occurred in the aftermath of the Data Breaches and are directly tied to information compromised in those attacks. Defendants' challenges to Plaintiffs' standing should be rejected.

The complaint describes OPM's considered failure over the course of several years to implement security directives from its Office of Inspector General ("IG") as to data security measures that would have brought OPM's systems into compliance with federal law and safeguarded the information under OPM's control. OPM repeatedly violated federal law in spite of earlier intrusions and millions of new intrusion attempts every month, rendering it amenable to suit under the Privacy Act and the Administrative Procedure Act. KeyPoint's immunity defense fails because it departed from its governmental mandate by unreasonably failing to protect the information entrusted to it and the security credentials needed to access its and OPM's systems. As alleged in the complaint, KeyPoint's failure to protect its credentials resulted in their being stolen and used by intruders to penetrate OPM's systems.

Defendants' remaining challenges to the complaint should be rejected. OPM is liable under the Privacy Act for intentionally and willfully failing to protect Plaintiffs' information. Relief under the Administrative Procedure Act is warranted in light of OPM's ongoing failure to establish data security defenses in compliance with binding federal standards. The complaint states a claim for negligence by alleging that KeyPoint breached its duty to take reasonable precautions to protect Plaintiffs' information from foreseeable harm. Further, the complaint alleges that, as a result of KeyPoint's failure to secure its systems, KeyPoint furnished Plaintiffs' private facts to hackers in a highly offensive manner, in violation of the Fair Credit Reporting Act and Plaintiffs' privacy rights. The complaint also alleges KeyPoint's violations of state statutes prohibiting unfair trade practices and requiring prompt disclosure of data breach incidents. Finally, the complaint alleges that OPM and KeyPoint acted deceptively and breached contractual promises to federal job applicants that their information would be held in confidence.

For the reasons set forth below, Plaintiffs respectfully submit that the Court should deny Defendants' motions to dismiss.

SUMMARY OF FACTUAL ALLEGATIONS

A. OPM's Inadequate Data Security

OPM oversees more than two million federal background and security clearance investigations annually, and it contracts with KeyPoint to perform the majority of its investigative work in the field. Consolidated Am. Compl. ¶¶ 52–53, 60, 75 (Mar. 14, 2016) ("Compl."). [Dkt. No. 63.] OPM collects and maintains—and KeyPoint has access to—millions of personnel files that include names, birthdates, Social Security numbers, fingerprint records, and detailed personal, medical, financial, and associational histories. *Id.* ¶¶ 61, 76, 129, 140,

144. OPM and KeyPoint promised federal employees, contractors, and job applicants that the confidentiality of their personal information would be preserved. *Id*. ¶¶ 68–70, 77.

The IG performs annual audits of OPM's information security to test and ensure compliance with federal requirements. Compl. ¶ 84. In each audit conducted from 2007 to 2015, the IG determined that OPM's information security policies and practices contained significant, material deficiencies posing an immediate threat to the security of assets or operations. *Id.* ¶¶ 86–89. Among other violations, OPM operated numerous electronic systems lacking valid security authorizations, failed to implement multi-factor authentication for accessing systems, failed to continuously monitor systems for security events, failed to patch and segment systems, and failed to implement centralized data security protocols and governance. *Id.* ¶¶ 90–113. In November 2014, the IG advised OPM to shut down all systems lacking current and valid authorization. *Id*. ¶ 103.

B. The Cyberattacks on KeyPoint and OPM

On November 1, 2013, hackers infiltrated OPM's network and stole documents showing how OPM's information systems were structured. Compl. ¶ 125. Then in December 2013, hackers breached the systems of two OPM contractors, including KeyPoint. *Id.* ¶ 114. KeyPoint did not detect the breach of its systems (the "KeyPoint Breach")—which compromised the sensitive personal information of over 48,000 people—until September 2014. *Id.* ¶¶ 117, 120. After learning of the KeyPoint Breach, OPM did not limit or terminate KeyPoint's access to its systems, despite the direct connections between its systems and those of KeyPoint. *Id*. ¶¶ 76, 119, 217. OPM instead arranged for KeyPoint to perform additional background checks. *Id.* ¶¶ 116, 119. KeyPoint increased its workforce to accommodate the increased workload, but did not simultaneously increase managerial oversight to keep pace with that growing workforce. *Id.*

Using log-in credentials stolen from KeyPoint, hackers breached OPM's network on May 7, 2014. Compl. ¶ 127. They installed malware and extracted the personal information of millions of people who had undergone federal background checks as well as the information of millions of their family members and cohabitants, including 5.6 million sets of fingerprints. *Id.* ¶¶ 127, 140–41. OPM's systems were breached again in or around October 2014, resulting in further theft of the personal information of another 4.2 million people. *Id.* ¶¶ 131, 138–39. OPM failed to detect these breaches for nearly a year, during which time the hackers had free rein within OPM's network. *Id.* ¶¶ 129, 133–34. OPM announced these breaches (the "OPM Breaches") in June and July 2015. *Id.* ¶¶ 138–41.

After the Data Breaches were disclosed, OPM offered free fraud monitoring and identity theft protection services to individuals whose personal details, such as birthdates, Social Security numbers, and fingerprints, were stolen. Compl. ¶¶ 148–50. Although this theft puts an individual at risk throughout her lifetime, OPM's remedial offer was limited to either 18 months or three years. *Id.* ¶ 150.

C. OPM's Ongoing Cybersecurity Deficiencies

Even after the Data Breaches OPM did not improve its cybersecurity. The IG's latest audit, in November 2015, found that a lack of compliance still "seems to permeate" OPM's information security regime, and that "OPM continues to fail to meet FISMA requirements" and had not followed most of the IG's prior directives. Compl. ¶ 152. For example, up to 23 of OPM's systems were still operating without valid authorizations, and none of OPM's major applications required the multi-factor authentication required by federal law. *Id.* ¶¶ 153–57. On February 10, 2016, the IG informed OPM that actions taken by its acting director are void, and

that "these actions may be open to challenges before the federal district court for the District of Columbia." *Id*. ¶¶ 158–62.

D. Plaintiffs' Economic Injuries in the Wake of the Data Breaches

Soon after KeyPoint's and OPM's systems were breached, Plaintiffs began to experience incidents of fraud and identity theft associated with the personal information that was stolen. First, their personal accounts incurred unauthorized debits, which Plaintiffs spent time trying to get resolved, not always successfully. *E.g.*, Compl. ¶¶ 13, 19, 29–31, 38, 41, 49, 50. Second, loans were fraudulently taken out and credit cards fraudulently opened under Plaintiffs' identities, causing them to incur pecuniary loss for false debts and lost time to contest the fraud. *E.g.*, *id.* ¶¶ 22, 28, 31, 45, 49. Third, tax returns were fraudulently filed using Plaintiffs' identities, causing them to incur costs and forgo possession of tax refund payments for months or years until the completion of the relevant tax authorities' investigations. *E.g.*, *id.* ¶¶ 14, 24, 26, 28. Fourth, the identities of Plaintiffs' children were stolen, also causing out-of-pocket loss. *E.g.*, *id.* ¶¶ 31, 50. All of these incidents resulted from the Data Breaches; all cost Plaintiffs time and money. *E.g.*, *id*. ¶ 163.

LEGAL STANDARD

In ruling on Defendants' motions, the Court accepts the truth of the complaint's allegations, construes them as a whole, and resolves all inferences in Plaintiffs' favor. *Metropolitan Wash. Airports Auth. v. Citizens for Abatement of Aircraft Noise, Inc.*, 501 U.S. 252, 264 (1991) (Rule 12(b)(1)); *American Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (Rule 12(b)(1)); *Atherton v. D.C. Office of Mayor*, 567 F.3d 672, 677 (D.C. Cir. 2009) (Rule 12(b)(6)).

Although Defendants' arguments for dismissal here rely on extraneous material,[1] the 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." *Singh v. McHugh*, No. CV 14-1906 (ABJ), --- F. Supp. 3d ----, 2016 WL 2770874, at *9 (D.D.C. May 13, 2016) (Jackson, J.) (quotation marks and citation omitted).[2]

A cause of action requires only "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2); *Erickson v. Pardus*, 551 U.S. 89, 93 (2007). While they have done so here, Plaintiffs were not required to plead "detailed factual allegations" to state their claims. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Erickson*, 551 U.S. at 93 ("Specific facts are not necessary; the statement need only give the defendant fair notice of what the claim is and the grounds upon which it rests.") (citations and alteration omitted). Plaintiffs need only set forth enough facts to state claims that are facially plausible. *Rudder v. Williams*, 666 F.3d 790, 794 (D.C. Cir. 2012). "Indeed it may appear on the face of the pleadings that a recovery is very remote and unlikely but that is not the test." *Simms v. District of Columbia*, 699 F. Supp. 2d 217, 222 (D.D.C. 2010) (citation omitted). The standard calls only

[1] It is inappropriate for Defendants to challenge the sufficiency of the complaint on the basis of factual material not referenced in it. This material is hearsay from other sources. Defendants make no request for judicial notice. *E.g.*, OPM Mot. at 21 (citing DOJ report), 24 (report of Treasury Inspector General), 25 (GAO report), 25–26 (statement on Social Security Administration website), 66 n.37 (statement on White House blog); KP Mot. at 9 n.5 (statement of United States Senator), 15–16 (DOJ report), 19 (FAQ sheet by Congressional Research Service).

[2] "If . . . matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment" and Plaintiffs "must be given a reasonable opportunity to present all the material that is pertinent to the motion." Fed. R. Civ. P. 12(d). Hence, to the extent Defendants rely on material outside the pleadings, and particularly material relating to information within their possession or control, that material should either be excluded or Plaintiffs given an opportunity to take discovery.

for "more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted).

ARGUMENT

I. PLAINTIFFS ALLEGE SUFFICIENT FACTS TO ESTABLISH ARTICLE III STANDING AT THE PLEADING STAGE.

A. The Individual Plaintiffs Allege Actual and Imminent Concrete Injuries Caused by Defendants That Are Redressable Here.

To satisfy the standing requirement of Article III, a plaintiff must allege: (1) "an injury in fact—a harm suffered by the plaintiff that is concrete and actual or imminent, not conjectural or hypothetical;" (2) "causation—a fairly traceable connection between the plaintiff's injury and the complained-of conduct of the defendant;" and (3) "redressability—a likelihood that the requested relief will redress the alleged injury." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998) (quotation marks and citation omitted). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice[.]" *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

Plaintiffs allege facts that plausibly establish each of these requirements.

1. Plaintiffs Adequately Allege Injury in Fact.

Plaintiffs allege concrete injuries that they already suffered. They also allege concrete injuries that they are likely to suffer in the future. Each of the various injuries alleged in the complaint constitutes injury in fact for purposes of Article III.

a. Plaintiffs Expended Time and Money to Respond to Actual Identity Theft and Account Fraud.

Plaintiffs suffered specific instances of identity theft and account fraud as a result of the Data Breaches, and paid money attempting to repair this damage. Plaintiff Jane Doe discovered twelve unknown accounts that were fraudulently opened in her name and placed in collection for

nonpayment. Compl. ¶ 22. In response, she paid approximately $198 to a credit repair law firm that assisted her in closing these accounts and removing them from her credit history. *Id*. Plaintiff Charlene Oliver suffered fraudulent charges to her credit and debit cards; she also received a letter from her electricity utility company stating that her account had been closed, was no longer in her name, and had incurred charges of $500. *Id*. ¶ 41. The electricity company purported to refund her deposit by sending a check made out to another individual, and has demanded that she pay an additional deposit of $390 to restore service. *Id*. This dispute remains unresolved, and in response to the various incidents of identity theft and fraud, Oliver is paying $100 each month to a credit repair law firm to restore her credit. *Id*.

Adding to these out-of-pocket expenses, Plaintiffs devoted substantial time to closing fraudulent accounts and repairing damage to their credit in the aftermath of the Data Breaches. *E.g*., Compl. ¶ 13 (ten hours communicating with bank), ¶ 19 (ten hours speaking with bank and reviewing and submitting affidavits), ¶ 39 (many hours spent attempting to resolve multiple instances of fraud), ¶ 22 (between 40 and 50 hours dealing with fraudulent accounts, communicating with the FBI, and attempting to gain access to TransUnion credit report). As Seventh Circuit Chief Judge Diane Wood recently held, and as other recent decisions confirm, the "time and effort" a data breach victim reasonably expends in "monitoring both his card statements and his other financial information" may be "sufficient" to "support Article III standing." *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965–69 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015); *see also In re Anthem, Inc. Data Breach Litig.*, MDL No. 2617, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) ("Plaintiffs['] attempts to respond to this imminent threat—whether by paying out of pocket for credit monitoring or by using their own time for credit monitoring—resulted in damages that

may be recoverable."); *In re Zappos.com, Inc., Customer Data Security Breach Litig.*, MDL No. 2357, 2016 WL 2637810, at *4 (D. Nev. May 6, 2016) (plaintiffs' allegations of "use of their credit, harm to their credit, lost time spent closing fraudulent accounts, and lost funds and business due to fraudulent charges" conferred standing).

Furthermore, the IRS notified several of the Plaintiffs that their private information was used to file fraudulent tax returns to steal their tax refunds. Plaintiff Paul Daly learned that tax returns had been fraudulently filed using his and his wife's names and personal information, and he "has spent many hours attempting to resolve these tax fraud issues, which remain under investigation by the Internal Revenue Service." Compl. ¶ 21. Plaintiff Orin Griffith likewise "has spent several hours attempting to resolve [a fraudulently filed 2014 tax return]. Payment of his tax refunds was delayed for almost ten months." *Id*. ¶ 32. Thus, one effect of the Data Breaches was to deny several Plaintiffs access to their tax return funds. Such injuries resulting from fraudulent tax returns, including the time and expense incurred to resolve these issues with the IRS, readily meet the injury-in-fact requirement. *See, e.g.*, *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (allegations that fraudulent tax returns were filed, and that economic damages ensued, sufficed to survive a motion to dismiss); *Longenecker-Wells v. BeneCard Servs., Inc.*, No. 1:15-CV-00422, 2015 WL 5576753, at *4 (M.D. Pa. Sept. 22, 2015) ("Confronted with the allegations that fraudulent tax returns have already been filed in their names, we find that the other alleged injuries, or harms"—which the court identified as "filing fees, accounting costs, and identity theft protection"—"satisfy the 'injury-in-fact' prong to demonstrate standing to sue in the data-breach scenario we encounter here.").

Several Plaintiffs also allege that they spent substantial time and money responding to

unauthorized use of their Social Security numbers after the Data Breaches. *E.g.*, Compl. ¶ 41 (after her Social Security number was used to open accounts and hijack existing accounts, Oliver "purchased credit monitoring and repair services through a credit repair law firm, for which she pays $100 per month."), ¶ 14 ("Bachtell has devoted many hours to . . . placing a freeze on his credit and communicating with the Social Security Administration to terminate the unauthorized accounts."), ¶ 50 ("Winsor has spent approximately twelve hours attempting to resolve the fraudulent transactions and the misuse of her son's Social Security number.").

OPM seeks to disprove Plaintiffs' particularized economic injuries with a factual inference unsupported by the complaint—that Plaintiffs were or may be reimbursed for their losses. *See* OPM Mot. at 20. OPM cannot rely on any such inference, which is without basis and insufficient to defeat standing: "Although some credit card companies offer some customers 'zero liability' policies, under which the customer is not held responsible for any fraudulent charges, that practice defeats neither injury-in-fact nor redressability." *Neiman Marcus*, 794 F.3d at 697.

> The "zero liability" feature is a business practice, not a federal requirement. . . . Debit cards . . . receive less protection than credit cards. . . . If a person fails to report to her bank that money has been taken from her debit card account more than 60 days after she receives the statement, there is no limit to her liability and *she could lose all the money in her account*. In any event, as we have noted, reimbursement policies vary. For the plaintiffs, a favorable judicial decision could redress any injuries caused by less than full reimbursement of unauthorized charges.

Id. (emphasis added).

OPM's reliance on *Whalen v. Michael Stores Inc.*, No. 14-cv-7006, --- F. Supp. 3d ----, 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015), is undercut by the fact that the plaintiff has taken an appeal to the Second Circuit. *See Whalen v. Michael Stores Inc.*, No. 16-352 (2d Cir.) (appeal

filed Feb. 5, 2016). Moreover, while OPM contends that the district court in *Whalen* took "judicial notice of the fact that every major card issuer in the country has a zero-liability policy" (OPM Mot. at 20), that court did not say that it was taking judicial notice of anything. Nor are the policies of credit card issuers the sort of indisputably accurate facts that are the proper subject of judicial notice under Federal Rule of Evidence 201—let alone on a motion to dismiss.[3] Defendants here make no request for judicial notice and there is no basis to surmise that any "zero-liability policies" work so flawlessly that consumers suffer *no* injury when they experience financial account fraud like that alleged in Plaintiffs' complaint. Any evidentiary record developed on this issue would show that, even under such policies, consumers are required to spend time monitoring their statements and reporting fraudulent charges within a short time frame; that it is not always easy to discern a fraudulent charge; that card issuers do not necessarily accept the consumer's statement that he or she did not make the charge; and that the process of contesting fraudulent charges takes time and does not always go smoothly or result in success for the consumer.

Beyond asking this Court to draw contrary (impermissible) factual inferences, OPM's reimbursement argument errs by conflating injury with damages. That some Plaintiffs may have been, or in the future may be, reimbursed for their losses would not change the fact that, as

[3] OPM's other district court cases are no more persuasive. *See* OPM Mot. at 19–20. *Burton v. MAPCO Express, Inc*., 47 F. Supp. 3d 1279 (N.D. Ala. 2014), has been deemed bad law insofar as it held that "a victim of identity theft *must* allege . . . that he/she suffered an un-reimbursed or out-of-pocket expense, and this court will not so hold." *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (emphasis in original). No "binding" authority supports such a holding, and it would be "difficult to reconcile" with circuit court precedent. *Id*. *Hammond v. The Bank of New York Mellon Corp.* involved a ruling at summary judgment after discovery showed that only two people suffered unauthorized charges. No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010).

alleged in the complaint, Plaintiffs suffered injuries—which occurred and were complete at the point of loss. *See In re Nexium Antitrust Litig.*, 777 F.3d 9, 27 (1st Cir. 2015) ("In contemplation of law the claim for damages arose at the time the extra charge was paid. Neither the fact of subsequent reimbursement . . . nor the disposition which may hereafter be made of the damages recovered is of any concern to the wrongdoers.") (citing *Adams v. Mills*, 286 U.S. 397, 407 (1932)). Any reimbursement Plaintiffs might subsequently obtain from third parties would at most be relevant to the measurement of damages. Such reimbursements or setoffs do not annul, but stand apart from, Plaintiffs' Article III injuries. *See, e.g.*, *Hearts with Haiti, Inc. v. Kendrick*, No. 2:13-CV-00039-JAW, 2015 WL 4065185, at *2 (D. Me. July 2, 2015) (courts "have stated on a number of occasions that a plaintiff suffers a pecuniary loss even if the loss could have passed through to a third party."); *In re Checking Account Overdraft Litig.*, 307 F.R.D. 630, 643 (S.D. Fla. 2015) (plaintiff who incurred excess fees because of a bank's wrongful scheme, but who was not entitled to damages because the bank closed his account with a negative balance, remained typical of the class); *In re Enron Corp. Sec., Deriv. & "ERISA" Litig.*, 310 F. Supp. 2d 819, 831 (S.D. Tex. 2004) ("[I]t is not necessary that a disclosure and subsequent drop in the market price of the stock have actually occurred, because the injury occurs at the time of the transaction") (citation omitted).

Nor does OPM's claim that financial fraud has affected "only a small subset of 15 individual Plaintiffs" (OPM Mot. at 21) have any legitimacy. *See also* KP Mot. at 16. Fifteen Plaintiffs are more than enough, and there is no basis to presume that their experiences constitute the full scope of harm suffered by the victims of the Data Breaches. Rather, the complaint alleges these Plaintiffs' experiences are representative and typical. Compl. ¶¶ 169–70.

b. Plaintiffs Incurred Monitoring Costs to Mitigate the Increased Risk of Identity Theft Caused by the Data Breaches.

Following the announcement of the Data Breaches, several Plaintiffs purchased credit monitoring services and, where identity theft incidents had already occurred, restoration and repair services. For example, Plaintiff John Doe II pays $329 annually for credit monitoring services. Compl. ¶ 25. Daly spends $29.95 per month for credit monitoring services to protect against identity theft. *Id*. ¶ 21. Oliver pays $100 a month to a law firm that monitors her identity and works to repair the damage done to her credit. *Id*. ¶ 41.

These costs, incurred as a consequence of a data breach, are concrete injuries for Article III purposes. *Neiman Marcus*, 794 F.3d at 694 (credit monitoring costs "easily" qualified as Article III injury); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164–65 (1st Cir. 2011) (costs of credit monitoring services held cognizable injuries following a "sophisticated breach of electronic data"); *Lambert v. Hartman*, 517 F.3d 433, 438 (6th Cir. 2008) (monitoring costs incurred to mitigate identity theft risks satisfied Article III); *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205-R, 2012 WL 2873892, at *5–11 (W.D. Ky. July 12, 2012) (same).

OPM counters with the Supreme Court's statement that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." OPM Mot. at 30 (citing *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1151 (2013)). But *Clapper* was not a data breach case and does not speak to what constitutes a "risk of real harm" in this factual setting. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016). The Court did state that "[i]n some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Clapper*, 133 S. Ct. at 1150 n.5. *Clapper* held that out-of-pocket costs are insufficient to support Article III standing where it is not clear that the harm-

inducing event has even occurred—in that case, allegedly unconstitutional surveillance. *Id.* at 1151–52. *Clapper* did not address situations in which the harmful events—like the Data Breaches here—indisputably have occurred.

Thus, "[i]t is important not to overread *Clapper*." *Neiman Marcus*, 794 F.3d at 694. "*Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place. An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring." *Id.*; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) ("Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real.") (citation omitted).

OPM also claims that Plaintiffs may not recover their out-of-pocket losses for identity theft protection services on the grounds that they bought those services after OPM offered its own batch of services. *See* OPM Mot. at 31. But OPM's argument is based on the unsupported inferences that (1) Plaintiffs paid for their services after, rather than before, OPM's remedial offer, and (2) the services Plaintiffs purchased provide no greater protection than the services being offered by OPM. Compl. ¶¶ 138–42, 148–51. OPM is not entitled to these inferences. Moreover, the fact that OPM offered a "comprehensive suite" of identity theft services for a limited time period (OPM Mot. at 8, 31, 42) demonstrates OPM's own recognition of risk. "It is unlikely that [OPM] did so because the risk is so ephemeral that it can safely be disregarded." *Neiman Marcus*, 794 F.3d at 694.

Faced with the prospect of identity theft—an injury that often takes years to remedy and sometimes can never be fully repaired—Plaintiffs reasonably paid to protect themselves.

c. Plaintiffs Face a Concrete, Impending Risk of Identity Theft.

As explained above, Plaintiffs allege concrete, actual injuries that have already occurred, thus satisfying the requirements of Article III. The heightened risk of additional, similar injuries in the future to Plaintiffs and the vulnerable class members also satisfies Article III.

The most recent standing decisions of the Supreme Court hold that while "Article III standing requires a concrete injury even in the context of a statutory violation," "[t]his does not mean . . . that the *risk of real harm* cannot satisfy the requirement of concreteness." *Spokeo*, 136 S. Ct. at 1549 (emphasis added). On one hand, "fears of hypothetical future harm that is not certainly impending," or fears of harm absent a "'substantial risk' that the harm will occur," do not satisfy the requirement of concreteness. *Clapper*, 133 S. Ct. at 1150–51 & n.5. But, unauthorized disclosure of names, addresses, Social Security numbers, fingerprints, and information about financial accounts, debts, bankruptcy filings, and credit ratings (Compl. ¶¶ 141, 144) creates a concrete and impending "risk of real harm." *Spokeo*, 136 S. Ct. at 1549.

OPM asserts that the courts that have found Article III standing in data breach cases are "in the clear minority[.]" OPM Mot. at 29. To the contrary, the majority of the circuits to have addressed the question found that an increased risk of identity theft constitutes injury in fact for Article III purposes. *See, e.g.*, *Neiman Marcus*, 794 F.3d at 692–94; *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010); *Lambert*, 517 F.3d at 438; *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007); *cf. Hannaford Bros.*, 659 F.3d at 164 (finding "a real risk of misuse" supported standing based on mitigation costs); *but see Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (no allegations of any data misuse). Particularly in light of

Spokeo's recognition that "risk of real harm" may confer standing, 136 S. Ct. at 1549, Defendants cannot credibly impugn the data breach decisions of the Seventh, Sixth, First, and Ninth Circuits on the grounds that some of them predate *Clapper*. *See* John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 Minn. J. L. Sci. & Tech. 943 (2016) (noting that this lopsided circuit split survived *Clapper* and explaining that standing normally exists in data breach cases based upon the threat of future harm, as well as reasonable measures taken to counteract such harm). *Spokeo* confirms that injured persons have standing to sue when they have suffered—or are at risk of suffering—a harm tethered to real-world concerns or generally recognized at common law. 136 S. Ct. at 1548–50.

A heightened risk of identity theft constitutes actionable harm in and of itself. *Krottner*, 628 F.3d at 1143; *Pisciotta*, 499 F.3d at 634; *see also Spokeo*, 136 S. Ct. at 1549 ("[I]ntangible injuries can nevertheless be concrete."). To be sure, some decisions have rejected standing where it is unlikely that stolen data has fallen into the hands of those able to misuse it. Defendants' principal cases (*see* OPM Mot. at 21–22; KP Mot. at 8–9) involved this sort of circumstance, *e.g.*, a "seemingly run-of-the mill theft" in which "a thief broke into a car sitting in a San Antonio parking garage and stole the car's GPS system, stereo, and several data tapes." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014). The *SAIC* court found no imminent injury because the thief in that case probably did not know what the data tapes were, nor was it likely that the thief could exploit them.

> First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. . . . Then, the criminal would have to find a tape reader and attach it to her computer. Next, she would need to acquire software to upload the data from the tapes onto a computer . . . . After that, portions of the data that

> are encrypted would have to be deciphered . . . . Once the data was fully unencrypted, the crook would need to acquire a familiarity with TRICARE's database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular Plaintiff's name and social security number (out of 4.7 million TRICARE customers) or sell that Plaintiff's data to a willing buyer who would then abuse it.

Id. at 25.

But when a data breach results, not inadvertently as part of a random burglary, but from a targeted and malicious attack, there is a risk of imminent injury that gives rise to standing. Standing thus existed in *Pisciotta*, where the "the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious." 499 F.3d at 632. Likewise, in *American Federation of Government Employees v. Hawley*, a hard drive containing private and sensitive employee information was stolen from a secure area within TSA headquarters, and the court found that individual plaintiffs had standing to sue under the Privacy Act. 543 F. Supp. 2d 44, 45, 50–51 (D.D.C. 2008).

Even courts that have held that a risk of future harm by itself is not a cognizable injury have recognized that this risk does constitute Article III injury when coupled with allegations of actual fraud or identity theft. *See Khan v. Children's Nat'l Health Sys.*, No. 8:15-cv-02125, --- F. Supp. 3d ----, 2016 WL 2946165, at *5 (D. Md. May 19, 2016) ("[I]n the data breach context, plaintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put 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."); *see also In re SuperValu, Inc. Customer Data Security Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *6–7 (D. Minn. Jan. 7, 2016), *appeal docketed*, No. 16-2528

(8th Cir. June 2, 2016); *In re Zappos.com, Inc. Customer Data Security Breach Litig.*, 108 F. Supp. 3d 949, 955 (D. Nev. 2015). If Plaintiffs here who have not yet experienced identity theft were forced to wait until they were defrauded or their identities stolen to pursue relief, their claims could end up time-barred. *See Adobe*, 66 F. Supp. 3d at 1215 ("[T]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact.") (citing *Clapper*, 133 S. Ct. at 1150 n.5).

The circumstances of this case are unlike those in *Reilly*, where the court held that employees of a customer of a payroll processing firm, whose system was hacked, lacked standing to sue. 664 F.3d at 40. In *Reilly* there was "no evidence that the intrusion was intentional or malicious," as "no evidence suggest[ed] that the data has been—or will ever be—misused" and it was "not known whether the hacker" had "read, copied, or understood" any information about the plaintiffs. *Id*. at 40, 43–44. The facts in *Reilly* differ materially from Plaintiffs' well-pled allegations of sophisticated, malicious targeting of their personnel files and incidents of misuse.

The OPM data theft was no ordinary burglary, as in *SAIC*. These attacks were "sophisticated, malicious, and carried out to obtain sensitive data for improper use." Compl. ¶¶ 117, 128, 132. The attacks were executed in stages over the course of several months and targeted to extract the government's sought-after files on its employees. *Id*. ¶¶ 114–33. Some individuals whose contact information was stolen in the Data Breaches even received unauthorized duplicates of OPM's notification e-mails with false links asking them to divulge additional information. *Id.* ¶ 148.

OPM's argument disregards the allegations of the complaint, making the false

assumption that this is one of the "data security breach cases where plaintiffs' data has not been misused . . . ." OPM Mot. at 27 (citation omitted). But Plaintiffs allege a range of incidents that embody several forms of injurious data misuse. And the misuse detailed in the complaint strongly supports the allegations that these attacks targeted private information for improper use. Given these real-world circumstances, the risk of identity theft confronting all Plaintiffs and class members cannot be dismissed as "conjectural or hypothetical" in nature. There is no reason to believe the class representatives are prone to irrational fears. *Cf.* Compl. ¶¶ 24–25, 37. Tellingly, after questioning the reasonableness of Plaintiffs' concerns that the Data Breaches have placed them and their minor children in harm's way, OPM admits it has offered identity protection services for the minor children. *See* OPM Mot. at 32–33 n.23.

d. Plaintiffs Face an Increased Risk of Bodily Injury or Death.

Defendants also fail to address Plaintiffs' allegations that several of the Plaintiffs and their families face an increased risk of bodily injury or death as a result of the Data Breaches. For example, Plaintiff Jane Doe II's husband is an Assistant United States Attorney who prosecutes large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families. Compl. ¶ 23. The Data Breaches exposed personal information of both Doe II and her husband that criminal elements could use to target them for harm. *Id.*; *see also id.* ¶ 13 (Plaintiff Travis Arnold, a former artillery operator, "suffers stress related to concerns for his personal safety and that of his family members"), ¶ 22 (the FBI informed Plaintiff Jane Doe that her sensitive personal information has been acquired by the rogue state known as ISIS).[4]

[4] OPM's claim that these injuries are not fairly traceable to the OPM Breaches (OPM Mot. at 32 n.23) fails for the reasons provided below. *See infra* Section I.A.2.

Even under the minority position, the risk of bodily injury or death would constitute an Article III injury. As the Third Circuit observed in *Reilly*, while a risk of financial injury could be redressed should it come to pass in the future, an increased risk of injury or death could not: "Waiting for a plaintiff to suffer physical injury before allowing any redress whatsoever is both overly harsh and economically inefficient. The deceased, after all, have little use for compensation." 664 F.3d at 45 (quotation marks and citation omitted). Courts therefore "resist strictly applying the 'actual injury' test when the future harm involves human suffering or premature death." *Id*.

e. Plaintiffs Have Suffered, and Continue to Suffer, Emotional Distress.

Many of the Plaintiffs allege that they suffer emotional stress as a result of the Data Breaches. *E.g.*, Compl. ¶ 18 ("[Brown] suffers stress resulting from fear that the theft of her sensitive personal information will impair her ability to obtain future federal government employment or security clearances, and fear for the safety of her family members who serve in the military."), ¶ 19 ("[Burnett-Rick] suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future and concerns that her fingerprints and sensitive personal information will be used to commit identity theft."), ¶ 30 ("[Gonzalez] suffers stress resulting from concerns that his exposure to the Data Breaches will impair his ability to renew his current security clearance and/or to obtain a higher security clearance in the future."). Such emotional distress caused by a data breach constitutes injury in fact. *In re Dep't of Veterans Affairs Data Theft Litig.*, No. 06-0506, 2007 WL 7621261, at *3 (D.D.C. 2007) ("*VA Data Theft*") (holding that "embarrassment, inconvenience, unfairness, mental distress, emotional trauma, pecuniary damages and the threat of current and future substantial harm from identity theft" constitute Article III injuries).

OPM claims that Plaintiffs' emotional distress is not a cognizable injury because the harms they fear are not sufficiently imminent to satisfy the requirements of Article III. *See* OPM Mot. at 31–33. In the cases that OPM cites, however, the facts alleged did not suggest any reasonable basis to fear that the plaintiffs' information would actually be misused. *See, e.g.*, *Reilly*, 664 F.3d at 44 (emotional distress did not constitute injury where "no identifiable taking" of the plaintiffs' information occurred); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *4–5 (N.D. Ill. Sept. 3, 2013) (emotional distress did not constitute injury absent "facts to support the allegations that the information was disclosed" in the first place); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848, at *3 (N.D. Cal. Nov. 11, 2011) (emotional distress found not a cognizable injury where no facts suggested the data could even be connected back to individual plaintiffs). By contrast where, as here, facts suggest the intrusion was intentional and malicious and exposed personal information to those willing and able to misuse it, courts have found that a plaintiff's emotional distress constitutes cognizable Article III injury. *See Pisciotta*, 499 F.3d at 632. In *Krottner*, for instance, the Court of Appeals held that emotional distress caused by the theft of a laptop containing Starbucks employees' names, addresses, and Social Security numbers constituted injury in fact. 628 F.3d at 1142.

For purposes of Plaintiffs' claim under the Privacy Act, "'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." *Doe v. Chao*, 540 U.S. 614, 624 (2004). Before the Supreme Court issued *FAA v. Cooper*, 132 S. Ct. 1441 (2012), courts in this circuit held that emotional distress satisfied the Privacy Act's threshold standing requirement of an "adverse effect." *Albright v. United States*, 732 F.2d 181, 186 (D.C. Cir. 1984); *Kvech v. Holder*, No. 10-cv-545, 2011 WL

4369452, at *4 (D.D.C. Sept. 19, 2011); *Hawley*, 543 F. Supp. 2d at 50–51 (plaintiffs suffered Article III adverse effects in the form of "embarrassment, inconvenience, mental distress, concern for identity theft, concern for damage to credit report, concern for damage to financial suitability requirements in employment, and future substantial financial harm [and] mental distress due to the possibility of security breach at airports."); *Krieger v. Department of Justice*, 529 F. Supp. 2d 29, 53 (D.D.C. 2008); *see also Speaker v. HHS Ctrs. for Disease Control & Prevention*, 623 F.3d 1371, 1382–83 (11th Cir. 2010). *Cooper* requires a plaintiff to plead actual pecuniary loss to satisfy a substantive element of the *Privacy Act*. *Cooper* neither alters nor calls into question the case law holding that emotional distress constitutes injury in fact for purposes of *Article III*.

The DOJ's Privacy Act primer (currently available on its website) recognizes what its argument here does not:

> The threshold showing of "adverse effect," which typically is not difficult for a plaintiff to satisfy, should carefully be distinguished from the conceptually separate requirement of "actual damages," discussed below. See, e.g., Fort Hall Landowners Alliance, Inc. v. BIA, 407 F. Supp. 2d 1220, 1225 (D. Idaho 2006) (explaining that "[i]t is important not to confuse this standing requirement with the entirely separate element that requires proof of actual damages" and that "to satisfy the Privacy Act's adverse effect and causation requirements, plaintiffs need not show actual damages from the disclosure, but must merely satisfy the traditional 'injury-in-fact and causation requirements of Article III'").[5]

2. Plaintiffs' Injuries Are Fairly Traceable to Defendants' Conduct.

The second prong of Article III standing—traceability—requires plausible allegations of a causal nexus between the alleged injury in fact and the alleged violations. *See Steel Co.*, 523

[5] United States Department of Justice, Overview of the Privacy Act of 1974, *available at* https://www.justice.gov/opcl/civil-remedies.

U.S. at 103; *Lujan*, 504 U.S. at 560–61. "Importantly . . . we are concerned with something less than the concept of 'proximate cause.'" *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003); *Rothstein v. UBS AG*, 708 F.3d 82, 91 (2d Cir. 2013). Here, Plaintiffs allege that Defendants failed to secure their sensitive personal information (Compl. ¶¶ 78–113); that this information was stolen by hackers who gained access to Defendants' inadequately secured computer systems (*id*. ¶¶ 114–37, 143–47); and that Plaintiffs consequently were subjected to actual and imminent harm (*id*. ¶¶ 13–50, 163). Nothing further is required at this point to show that the harm is plausibly traceable to Defendants' misconduct. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that allegations that laptops containing personal information were not adequately secured and then were stolen, and that plaintiffs thereafter experienced identity theft, satisfied Article III requirements).

a. Plaintiffs Need Not Negate Potential Alternative Causes in the Operative Pleading.

OPM's speculation that Plaintiffs' information might have been exposed in unrelated data breaches, or perhaps from "rummaging through trash" (OPM Mot. at 25), does not render implausible the allegations that their injuries are traceable to Defendants' security failures. As recognized in the pair of data breach decisions written by Judge Wood for the Seventh Circuit, the source or sources of harm present a question of fact—whereas the complaint's allegations must be accepted as true for purposes of Rule 12. Accordingly, "[m]erely identifying potential alternative causes does not defeat standing." *P.F. Chang's*, 819 F.3d at 969.

> The fact that Target or some other store might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are "fairly traceable" to the data breach at Neiman Marcus.

Neiman Marcus, 794 F.3d at 696. These holdings follow the common law of torts, which, "in

multiple causation cases . . . has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring in the judgment) (citing *Summers v. Tice*, 199 P.2d 1, 3–4 (Cal. 1948)).

Defendants' argument regarding the prevalence of data breach incidents assumes that individuals who reported past exposure to data breach incidents were not excluded from the group of potential class representatives. Defendants are not entitled to adverse inferences, and "[t]raceability does not require that the defendants be the only cause of the injury." *United States v. Ramos*, 695 F.3d 1035, 1046 (10th Cir. 2012). If accepted, Defendants' argument also would "create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable." *Anthem*, 2016 WL 3029783, at *15.

Equally devoid of merit is KeyPoint's claim that because Plaintiffs allege KeyPoint and OPM together bear legal responsibility for harm occasioned by the Data Breaches, neither Defendant can be held liable. *See* KP Mot. at 12–14. The law is instead clear that when two defendants have breached a duty to the plaintiff, the burden shifts to the defendants to establish that their negligence was not a cause of the plaintiff's injuries. *Price Waterhouse*, 490 U.S. at 263 (O'Connor, J., concurring in the judgment). So too, the burden shifts "where the effect of a defendant's tortious conduct combines with a force of unknown . . . origin to produce the harm to the plaintiff." *Id*. (citations omitted); *accord Public Citizen Health Research Grp. v. Young*, 909 F.2d 546, 550 (D.C. Cir. 1990); Prosser & Keeton on the Law of Torts § 41 at 271 (5th ed.).

At bottom, Defendants' causation arguments would have this Court construe Plaintiffs' allegations against them, instead of accepting all well-pled allegations as true. Challenges to causation should be litigated on a more developed record. *See Spann v. Colonial Vill., Inc.*, 899

F.2d 24, 29 (D.C. Cir. 1990).

b. The Complaint Sufficiently Alleges a Causal Link Between KeyPoint's Inadequate Data Security and the Data Breaches.

According to KeyPoint, the injuries set forth in the complaint are not fairly traceable to KeyPoint's conduct because Plaintiffs do no more than "imply that the KeyPoint cyber-attack enabled hackers to access OPM's networks using stolen credentials." KP Mot. at 13. The complaint alleges that KeyPoint's conduct caused Plaintiffs' harm in two ways: (1) KeyPoint failed to implement sufficient data security measures to prevent cyber-attackers from accessing its systems, resulting in the personal information of 48,000 federal employees being compromised in the KeyPoint Breach (Compl. ¶¶ 4, 121–23); and (2) KeyPoint failed to implement secure log-in and authentication measures, which allowed cyber-attackers to steal KeyPoint user credentials and deploy them to access systems within OPM's network, resulting in the theft of more than 21 million people's information in the OPM Breaches (*id*. ¶¶ 1, 127, 133, 222–28). Based upon Plaintiffs' allegations that KeyPoint's derelict data security was a "but for" cause of both the KeyPoint Breach and the OPM Breaches, the injuries that Plaintiffs suffered as a result of these breaches are "fairly traceable" to KeyPoint's conduct. *See Edmonson v. Lincoln Nat'l Life Ins. Co*., 725 F.3d 406, 418 (3d Cir. 2013) (explaining that the "fairly traceable" requirement can be met "even where the conduct in question might not have been a proximate cause of the harm, due to intervening events.") (citation omitted).

KeyPoint strays from the complaint to opine that its credentials "could have been stolen at any time by any number of methods from any number of individuals." KP Mot. at 13. But how and why KeyPoint's credentials were stolen are factual questions that should be subject to discovery and resolved on a fully developed record. At the pleading stage, Plaintiffs' allegations, taken as true, are sufficient to demonstrate harm fairly traceable to KeyPoint.

See Anthem, 2016 WL 3029783, at *16 (defendants "never challenged the fact that (1) the Anthem Database was breached, (2) that this breach exposed the PII of approximately 80 million individuals, and (3) that the Anthem Database contained the PII of every single putative class member in the instant action. That is sufficient for purposes of pleading consequential injury"); *In re Target Corp. Data Security Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014); *Neiman Marcus*, 794 F.3d at 696 ("It is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach . . . . It is enough at this stage . . . that [defendant] admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk.").

c. The Information Used to Inflict Harm on Plaintiffs After the Data Breaches Is the Same Information That Was Stolen in the Data Breaches.

KeyPoint ignores the complaint's allegations when it asserts that Plaintiffs have not alleged what information they provided to Defendants, what information was compromised, or how this disclosure could have led to identity theft. *See* KP Mot. at 14–16. Plaintiffs' complaint specifies the information compromised in the Data Breaches. *E.g.*, Compl. ¶ 67 ("financial histories and investment records"), ¶ 144 ("Information about financial accounts, debts, bankruptcy filings, and credit ratings and reports"), ¶ 146 ("financial records that include bank account and credit card information"). Also specified is the information exploited to inflict injury upon various Plaintiffs. *E.g.*, *id*. ¶¶ 13–50. And the complaint alleges it was the breach of Defendants' inadequate data security defenses that caused this information to be disclosed and misused. *E.g.*, *id*. ¶¶ 163, 178, 223, 225.[6]

[6] In a footnote, OPM objects that the complaint does not identify which notice each Plaintiff received, and asserts that this information would permit OPM to ascertain the data breach

[Footnote continued on next page….]

In view of these factual allegations, a finding that Defendants are legally responsible for Plaintiffs' injuries is plausible. The cases Defendants cite demonstrate the sufficiency of the allegations here. For example, in the *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, it was implausible that the lone identity theft incident resulted from misuse of data that was not even exposed in the underlying breach. No. 13-7418 CCC, 2015 WL 1472483, at *8 (D.N.J. Mar. 31, 2015), *appeal docketed*, No. 15-2309 (3d Cir. June 1, 2015). In this case, the nature and the timing of the harm sustained by Plaintiffs make it plausible that the information used to perpetrate this harm was obtained from OPM and KeyPoint.

To take one of several examples, the information OPM illegally made available about Plaintiff Tony Bachtell *and* his wife was used to file fraudulent tax returns on behalf of Bachtell *and* his wife. Compl. ¶ 14. Because sensitive information about both Bachtells was compromised as a result of Defendants' violations, the fact that information about both of them was misused in a single incident, in the wake of the Data Breaches, makes it likely that the information was obtained from Defendants. Exactly the same thing happened to Plaintiff Daly

---

affecting each Plaintiff. OPM Mot. at 18 n.12. But OPM itself possesses that information and it is enough that Plaintiffs allege they received notice of the theft of their information from Defendants' systems. *Cf. Policemen's Annuity & Ben. Fund of City of Chi. v. Bank of Am., NA*, 943 F. Supp. 2d 428, 442 (S.D.N.Y. 2013) ("At the pleading stage, plaintiffs cannot be required to identify breaches of representations and warranties with respect to the individual loans in the specific trusts—such information is, at this stage, . . . uniquely in the possession of defendants. Rather, plaintiffs satisfy their burden where their allegations 'raise a reasonable expectation that discovery will reveal evidence' proving their claim.") (citation omitted), *abrogated in part on other grounds by Retirement Bd. of the Policeman's Annuity & Ben. Fund v. Bank of N.Y. Mellon*, 775 F.3d 154 (2d Cir. 2014). Even in a fraud complaint subject to a heightened pleading standard, multiple defendants need to be informed of the allegations against them individually only "to the extent that such information is not uniquely within defendants' possession." *Gandhi v. Sitara Capital Mgmt., LLC*, 689 F. Supp. 2d 1004, 1008 (S.D.N.Y. 2010). The details of how Defendants' computer systems were breached, what information was stolen as part of each breach, which Plaintiffs were affected by each breach, and who may have stolen that information are uniquely available to Defendants and should be subject to discovery.

and his wife, a former IRS employee. *Id*. ¶ 21. Similarly, within months of the OPM Breaches, Plaintiff Kelly Flynn's and her husband's sensitive information was used to file fraudulent tax returns in their names and to take out payday loans. *Id*. ¶ 28. And it was in late 2014 and early 2015, shortly after the OPM Breaches began, that Plaintiffs Lilian Gonzalez-Colon and Orin Griffith experienced account and tax fraud. *Id*. ¶¶ 31, 32. Beginning in mid-2015, multiple inquiries were made on Plaintiff Alia Fuli's credit, and ultimately in December 2015 a credit card account was fraudulently opened in her name and used to make unauthorized purchases. *Id.* ¶ 29. And it was also during this time that Plaintiff Oliver's utility account was seized by a third party who had her Social Security number and maiden name—information she provided in order to serve in the Navy. *Id.* ¶ 41. The connection between violation and harm here is not remote.

3. Plaintiffs' Injuries Would Be Redressed by the Relief They Seek.

As indicated above, Plaintiffs allege concrete past injuries in the form of tax fraud, unauthorized credit card charges, debits to their bank accounts, lost security deposits, fraud on their utility accounts, credit monitoring and repair costs, emotional distress, and time spent responding to such incidents of misuse. *E.g.*, Compl. ¶¶ 13, 19, 21, 28–30, 38, 41–44. The damages that Plaintiffs seek under the Privacy Act, the Little Tucker Act, and various state laws would compensate them for their injuries.

The redressability prong of constitutional standing considers the likelihood that a favorable decision will provide a benefit to the plaintiff. *Steel Co.*, 523 U.S. at 103; *Lujan*, 504 U.S. at 561. While "not a demand for mathematical certainty," redressability asks for a "substantial likelihood" that the injury can be remedied in a judicial forum. *Freeman v. Corzine*, 629 F.3d 146, 153–54 (3d Cir. 2010) (citing, *inter alia*, *Vermont Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 771 (2000)).

Defendants venture outside the complaint to argue that redressability is not met on the grounds that third parties might reimburse Plaintiffs for their pecuniary harm. *See* OPM Mot. at 20–21; KP Mot. at 10 n.6, 16–17. OPM claims "Plaintiffs never allege that any of this fraudulent activity caused them actual monetary loss" absent allegations that their injuries were unreimbursed. OPM Mot. at 19. KeyPoint claims Plaintiffs nowhere allege "that they have had to pay [certain] amounts or that they remain outstanding . . . ." KP Mot. at 17 (alteration in original) (citation omitted). These arguments contradict the complaint and misstate the law.

First, the complaint alleges that Plaintiffs have suffered concrete injury in the form of unauthorized charges and deductions from their bank accounts. It is common sense that an award of damages can redress these injuries. Defendants' position that Plaintiffs must further allege their injuries have not been reimbursed to have standing is incorrect. It is well established that "[p]ayments made to or benefits conferred on the injured party from other sources are not credited against the tortfeasor's liability, although they cover all or a part of the harm for which the tortfeasor is liable." Restatement (Second) of Torts § 920A(2); *see also Board of Trs. of Hotel & Rest. Emps. Local 25 v. JPR, Inc.*, 136 F.3d 794, 805 n.13 (D.C. Cir. 1998). Far from requiring plaintiffs to plead that their injuries have not been reimbursed, "the common law 'collateral source rule,' recognized by the D.C. Circuit, would *preclude consideration* of payments from a source unrelated to defendants on the theory that the windfall of such a source should accrue to the victims rather than the tortfeasors." *Estate of Doe v. Islamic Republic of Iran*, 943 F. Supp. 2d 180, 186 (D.D.C. 2013) (emphasis added) (citation omitted).

Second, the complaint alleges that Plaintiffs incurred out-of-pocket damages. *E.g.*, Compl. ¶¶ 13, 22, 28, 30, 38, 39, 41, 49. Even if Defendants were correct that discovery might reveal some of these fraudulent charges to be reimbursed or reimbursable, Plaintiffs are unaware

of any credit card issuer, bank, or federal agency that would reimburse them for their out-of-pocket remediation costs, or for the time and effort needed to secure reimbursements. Defendants' speculative argument about "zero-fraud-liability policy" (OPM Mot. at 20; KP Mot. at 16–17) fails to refute redressability much as it fails to disprove Plaintiffs' injuries in fact. *See supra* Section I.A.1.a. That some Plaintiffs' pecuniary losses may be reimbursable does not alter the redressable nature of these injuries.

Third, Plaintiffs allege that the adverse effects of the Data Breaches required them to devote significant time to closing fraudulent accounts and repairing their credit. *E.g.*, Compl. ¶ 13 (ten hours communicating with bank employees), ¶ 19 (ten hours speaking with bank employees and reviewing and submitting affidavits), ¶ 22 (between 40 and 50 hours dealing with the fraudulent accounts, communicating with the FBI, and attempting to gain access to credit report). Plaintiffs' lost time constitutes Article III injury that would be redressed by monetary compensation. KeyPoint itself admits that "'lost time' is generally considered a purely economic loss." KP Mot. at 40 n.34; *see also, e.g.*, *Neiman Marcus*, 794 F.3d at 692 (describing injury caused by "the aggravation and loss of value of the time needed to set things straight").

Finally, the equitable relief sought by Plaintiffs will serve to redress the significant risk of future identity theft and other harm that they confront. *See, e.g.*, *Franklin v. Massachusetts*, 505 U.S. 788, 803 (1992) (declaratory relief request satisfied redressability); *Swan v. Clinton*, 100 F.3d 973, 980 (D.C. Cir. 1996) (injunctive relief request satisfied redressability).

B. Plaintiffs Plead Facts Sufficient to Establish Standing to Pursue Declaratory and Injunctive Relief.

Plaintiffs plausibly allege that hackers will continue to exploit the weaknesses in OPM's data security and expose the sensitive information in its control to further theft and misuse. Compl. ¶¶ 7, 152–57, 206. OPM's brushing off of this danger in the face of millions of

confirmed intrusion attempts every month only highlights the need for judicial supervision. That cyber criminals will continue to attack OPM's vulnerable systems is as inevitable as water flowing through a sieve—yet OPM has shown a consistent refusal to take these threats seriously and plug the holes. OPM's ongoing failures and violations give Plaintiffs standing to seek prospective relief under the Administrative Procedure Act and the Court's inherent authority.

OPM's extensive reliance on *City of Los Angeles v. Lyons*, 461 U.S. 95 (1983), underscores OPM's underestimation of the continuing threat. *See* OPM Mot. at 34–35. The Supreme Court found that Lyons, who had suffered chokeholds at the hands of the Los Angeles Police Department, lacked standing to enjoin the police department's future use of chokeholds. The notion that Lyons himself would be put in a chokehold again in the future was highly unlikely and speculative, the Court explained. 461 U.S. at 108–10. Here, however, it is a practical certainty that hackers will continue to attack OPM's inadequately secured systems. The OPM Breaches have shown the hacker community that OPM's servers remain vulnerable. Plaintiffs have no alternative but to seek Court intervention considering OPM's ongoing failure to follow the security directives of its IG. Compl. ¶¶ 8, 152–57.

C. The AFGE Has Associational Standing to Seek Declaratory and Injunctive Relief on Behalf of Its Members.

OPM's challenge to AFGE's associational standing lacks merit. "[A]n association has standing to bring suit on behalf of its members when: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977). As AFGE meets each of these requirements, it has standing to seek equitable relief on its members' behalf. Compl. ¶ 12.

First, AFGE sufficiently alleges that its members would otherwise have standing to sue in their own right. AFGE's members have been injured as a result of the Data Breaches and have received AFGE's help to obtain "administrative leave to register for identity theft protection services," and to manage "other fallout from the OPM Breaches." Compl. ¶¶ 12, 163; *see Warth v. Seldin*, 422 U.S. 490, 511 (1975).

The second, "germaneness requirement is 'undemanding' and requires 'mere pertinence' between the litigation at issue and the organization's purpose." *Association of Am. Physicians & Surgeons, Inc. v. Texas*, 627 F.3d 547, 550 n.2 (5th Cir. 2010) (citation omitted); *see also Center for Sustainable Economy v. Jewell*, 779 F.3d 588, 597 (D.C. Cir. 2015). AFGE satisfies this requirement as well. Equitable relief to bring OPM's data security into compliance with federal law, provide lifetime identify theft protection to AFGE members whose information was stolen in the Data Breaches, and ensure indemnification of their future losses stemming from the Data Breaches, would further AFGE's goal of working "to ensure that its members' rights, including statutory and contractual rights, are honored and protected . . . ." Compl. ¶¶ 11, 213–15.

Third, the AFGE members who are also absent members of the proposed class need not participate in this lawsuit. "'[I]ndividual participation' is not normally necessary when an association seeks prospective or injunctive relief for its members," for in such a case "it can reasonably be supposed that the remedy, if granted, will inure to the benefit of those members of the association actually injured." *United Food & Commercial Workers Union Local 751 v. Brown Grp., Inc.*, 517 U.S. 544, 553–54 (1996); *Warth*, 422 U.S. at 515; *see also Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 809–10 (1985) (stating that "an absent class-action plaintiff is not required to do anything. He may sit back and allow the litigation to run its course, content in knowing that there are safeguards provided for his protection.").

II. THE COMPLAINT STATES A CLAIM UNDER THE PRIVACY ACT.

The Privacy Act creates a cause of action for an individual who has suffered "an adverse effect" from a federal agency's failure "to comply with any other provision of [the Privacy Act], or any rule promulgated thereunder." 5 U.S.C. § 552a(g)(1)(D). Under the Act, a plaintiff who suffered "actual damages" as a result of an "intentional or willful" violation of the Act "shall" recover an "amount equal to the sum of . . . actual damages sustained by the individual," with a $1,000 minimum. 5 U.S.C. § 552a(g)(4)(a). As described below, Plaintiffs sufficiently plead a claim for violations of the Privacy Act.

A. Plaintiffs Adequately Allege Actual Damages.

OPM does not dispute that "out-of-pocket monetary losses" satisfy the Privacy Act's "actual damages" requirement (OPM Mot. at 37), and many of the Article III injuries discussed above were out-of-pocket losses. OPM's assertion that "Plaintiffs never claim that the alleged misconduct caused them personal monetary loss" (OPM Mot. at 39) is flatly at odds with the complaint. Plaintiffs allege, with supporting detail, fraudulent charges to their credit or debit cards, funds deducted from their bank accounts without their authorization, stolen tax refunds, and that they paid service providers to monitor and repair the damage to their credit. *See supra* Sections I.A.1.a, b. Plaintiffs further allege that these injuries resulted from OPM's Privacy Act violations. Compl. ¶¶ 178, 185. The Court cannot disregard these allegations simply because OPM takes issue with them.

1. Plaintiffs' Allegations of Actual Damages Would Satisfy Rule 9(g).

OPM claims in a footnote that the heightened pleading standard of Federal Rule of Civil Procedure 9(g) applies to Privacy Act claims. *See* OPM Mot. at 39 n.26. OPM does not, and cannot, cite any case so holding. Instead, OPM cites the *Cooper* case in which the Court

reasoned by analogy to "the common-law torts of libel *per quod* and slander, under which plaintiffs can recover 'general damages,' but only if they prove 'special harm . . . .'" 132 S. Ct. at 1451 (citations omitted). The Court held that a Privacy Act plaintiff may "recover the statutory minimum of $1,000, presumably for any unproven harm," by "showing some pecuniary harm, no matter how slight," but cannot recover based solely upon "loss of reputation, shame, mortification, injury to the feelings and the like . . . ." *Id*. The Court did not hold that Rule 9(g) applies to Privacy Act claims.

Even if this Court were to hold that Rule 9(g) applies, Plaintiffs' complaint meets that standard. "[A]llegations of special damage will be deemed sufficient for the purpose of Rule 9(g) if they are definite enough to enable the opposing party to prepare his or her responsive pleading and a defense to the claim." 5A Charles A. Wright & Arthur R. Miller, *Federal Practice & Procedure* § 1311. Rule 9(g) requires only that the complaint "adequately notify both defendants and the Court as to the nature of the claimed damages." *Halperin v. Kissinger*, 542 F. Supp. 829, 832 (D.C. Cir. 1982) (citing *Schoen v. Washington Post*, 246 F.2d 670, 672 (D.C. Cir. 1957)). Plaintiffs' complaint does this with its particularized injury and causation allegations. *E.g.*, Compl. ¶¶ 13–50, 134–37, 163, 178, 185; *see also supra* Sections I.A.1, 2. It is entirely plausible (if not perfectly obvious) that a Plaintiff who had funds withdrawn from his or her bank account, or lost a tax refund, or paid for credit monitoring services in the aftermath of the Data Breaches suffered an out-of-pocket loss.

2. OPM's Assertion That Plaintiffs' Out-of-Pocket Remediation Costs Are Not Cognizable Fails as a Matter of Fact and Law.

OPM also claims that Plaintiffs' out-of-pocket remediation costs are not cognizable under the Privacy Act because they were for "prophylactic measures taken to protect against the future risk of financial fraud or other harm." OPM Mot. at 42. OPM is wrong for two reasons.

First, Plaintiffs incurred out-of-pocket costs not just to mitigate a real risk of future identity theft but also to respond to injuries they already sustained. Plaintiffs paid for, among other services, assistance in getting fraudulent charges reversed and their credit reports amended to reflect those reversed charges. *E.g.*, Compl. ¶¶ 22, 41. These measures were remedial, not prophylactic. Consequently, the associated expenses are "actual damages" even under OPM's narrow view.

Second, OPM's argument mischaracterizes the Privacy Act's "actual damages" requirement. Plaintiffs' out-of-pocket expenses incurred to avoid harm resulting from the Data Breaches constitute actual damages under the Privacy Act for the same reason these expenses constitute injuries in fact—they were reasonably incurred to prevent concrete and impending risks of harm. In *Beaven v. U.S. Department of Justice*, the DOJ similarly argued that money spent to avoid future harm from a breach was not recoverable because the costs resulted from "the plaintiffs' own apprehension[.]" No. 03 84 JBC, 2007 WL 1032301, at *28 (E.D. Ky. Mar. 30, 2007), *aff'd in part, rev'd in part & remanded on other grounds*, 622 F.3d 540 (6th Cir. 2010). The court rejected the argument, finding that out-of-pocket costs to guard against potential harm by monitoring financial accounts constituted actual damages because the costs were incurred to prevent harm from the disclosure of protected information. *Id*. The court further found that the DOJ's proposed construction of the Privacy Act was "hypertechnical" and "excessively narrow[.]" *Id*.

OPM next resorts to policy, arguing that a plaintiff "could always, and quite easily, manufacture actual damages—with its associated $1,000 statutory damage provision—by spending a few dollars on credit monitoring services, credit reports, or credit freezes." OPM Mot. at 42. But only those who spend money to protect against a concrete, impending threat—as

opposed to, for example, spending out of baseless fear—suffer "actual damages" within the Privacy Act. Plaintiffs here did not incur credit monitoring and repair costs to manufacture standing; they did so because they had already suffered identity theft, they learned their sensitive information had been compromised in a broad-scale attack, or both. Given that OPM itself has offered credit monitoring services, Plaintiffs' decision to incur similar costs can scarcely be deemed unreasonable. These out-of-pocket losses qualify as actual damages.

B. Plaintiffs Adequately Allege Their Losses Resulted from OPM's Privacy Act Violations.

Plaintiffs sufficiently allege that OPM's Privacy Act violations caused them to incur economic loss. The complaint charges OPM with willfully violating section 552a(e)(10) by failing "to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members." Compl. ¶ 182. The complaint further charges OPM with willful violations of section 552a(b) because it disclosed "Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose." *Id*. ¶ 183. Plaintiffs allege they "have sustained and will continue to sustain actual damages and pecuniary losses directly traceable to OPM's violations set forth above." *Id*. ¶ 185.

These allegations are plausible given the totality of factual material in the complaint, including the allegations linking the data stolen by reason of OPM's violations to the data used to inflict harm on Plaintiffs. *E.g.*, Compl. ¶¶ 13–50, 67, 144, 146, 163; *see supra* Section I.A.2.c. The Privacy Act requires nothing more at this stage. *Hill v. U.S. Dep't of Def.*, 70 F. Supp. 3d 17, 22 (D.D.C. 2014) (holding that a Privacy Act complaint "must only plausibly allege proximate causation."); *see also Sabre Int'l Sec. v. Torres Advanced Enter. Solutions, Inc*., 820

F. Supp. 2d 62, 75 (D.D.C. 2011) (noting that proximate cause calls for "some reasonable connection between the act or omission of the defendant and the damages which the plaintiff has suffered.") (citing *Brewer v. Islamic Republic of Iran*, 664 F. Supp. 2d 43, 54 (D.D.C. 2009)).

C. Plaintiffs Adequately Allege That OPM Willfully or Intentionally Violated Sections 552a(e)(10) and 552a(b) of the Privacy Act.

Plaintiffs seek damages under 5 U.S.C. §§ 552a(g)(1)(D) and 552a(g)(4) for OPM's violations of 5 U.S.C. §§ 552a(e)(10) and 552a(b). The detailed allegations that OPM (i) refused to heed persistent official warnings of material deficiencies in its data security, (ii) knew of the breaches of its information systems and of the systems of other government agencies and of OPM's contractors, and (iii) knew of the nonstop attempted cyberattacks on its systems, render it plausible that OPM violated these provisions willfully or intentionally.

1. Legal Standard for Evaluating Whether Conduct Is Willful or Intentional for Purposes of a Privacy Act Claim.

Notwithstanding OPM's efforts to elevate the meaning of "intentional or willful" so as to create a single, seemingly insurmountable standard (OPM Mot. at 43–44), "[t]he terms 'intentional' and 'willful'" are to be "interpreted in their context[.]" *Albright*, 732 F.2d at 189. The legislative history shows that "[t]he Act's requirement of 'intentional or willful' agency conduct is lower than the House standard of 'willful, arbitrary or capricious[.]'" Frederick Z. Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611, 625 (1984). As applied by the courts, "elements of recklessness often have been a key characteristic incorporated into a definition of willful and intentional conduct." *Moskiewicz v. USDA*, 791 F.2d 561, 564 (7th Cir. 1986) (analyzing Privacy Act standard).

The D.C. Circuit has articulated various standards for determining when an agency's conduct is "intentional or willful" under the Privacy Act. In *Hill v. U.S. Air Force*, the court held

that conduct "merely 'somewhat greater than gross negligence'" provides a basis for liability under the Act.[7] 795 F.2d 1067, 1070 (D.C. Cir. 1986) (citing *Parks v. IRS*, 618 F.2d 677, 683 (D.C. Cir. 1980) (citing 120 Cong. Rec. 40405, 40406 (1974)). In *Albright*, the court held that the Privacy Act's *mens rea* standard is satisfied by "committing the act without grounds for believing it to be lawful, or by flagrantly disregarding others' rights under the Act," 732 F.2d at 189, and in *Waters* the court recognized all three of these iterations as appropriate, 888 F.2d at 875. Finally, in *Maydak v. United States*, the court surveyed this body of precedent and held that governmental action or inaction is willful or intentional if it falls into any of four categories:

- so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful, or
- somewhat greater than gross negligence, or
- committed without grounds for believing them to be lawful, or
- in flagrant disregard of others' rights under the Act.

630 F.3d 166, 179–80 (D.C. Cir. 2010) (bullet points in original).

OPM ignores the disjunctive nature of these tests. OPM's conduct, moreover, meets any and all of them: it was patently unlawful, more egregious than gross negligence, committed without grounds for believing it lawful, and in flagrant disregard of Plaintiffs' rights.

2. The Complaint Plausibly Alleges That OPM Willfully or Intentionally Violated the Safeguards Provision, Section 552a(e)(10).

OPM would have this Court conclude on the pleadings that its conduct was not willful or

[7] OPM omits essential words from this holding of *Waters v. Thornburgh*, 888 F.2d 870 (D.C. Cir. 1989), *abrogated on other grounds by Doe v. Chao*, 540 U.S. 614 (2004). *See* OPM Mot. at 44. In full, the sentence partially quoted by OPM is: "On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed as *only somewhat* greater than gross negligence." *Waters*, 888 F.2d at 875 (emphasis added) (citing 20 Cong. Rec. at 40,406).

intentional because data security is "complex" and its "alleged decision not to immediately implement every recommendation in the OIG annual FISMA audit does not rise to the level of willful and intentional . . . ." OPM Mot. at 47–48. But the complaint does not allege that OPM's violations consist in a failure to implement "every" single IG directive "immediately." Instead, the complaint lays out OPM's failure to adopt *numerous* critical IG directives, *year after year*. An analogous scenario would be a bank entrusted with guarding valuable items in safe deposit boxes leaving its windows unlocked and its vault door open, refusing to repair visibly broken security cameras, and doing so even after it and other banks nearby had been robbed and federal banking inspectors had repeatedly warned it to overhaul its security for years.

Courts have found that a defendant's inaction and neglect can be as willful or intentional as any affirmative misconduct. "[A]n omission, like an affirmative act, can be the result of intent, and a failure to act may be just as willful and malicious as any affirmative act." *In re Schachter*, No. 05-35078, 2007 WL 2238293, at *5 (Bankr. S.D.N.Y. Aug. 1, 2007); *see Velez v. City of New London*, 903 F. Supp. 286, 292 (D. Conn. 1995) (upholding claims where government defendants' "alleged failure to act may have been intentional"). Such willful misconduct generally includes "the wrongful failure to act, without just cause or excuse, where the actor is aware"—as OPM was aware—"that the actor's conduct will probably result in injury." *Swasey v. West Valley City*, No. 2:13-CV-00768-DN, 2015 WL 500881, at *2 (D. Utah Feb. 5, 2015) (quotation marks and footnote omitted); *see also RSM, Inc. v. Herbert*, 466 F.3d 316, 322 (4th Cir. 2006).

OPM was repeatedly made aware that its failure to act was putting at risk the safety and security of millions of government employees, and the agency was directed by its IG to take action to fix its security failures. These directives were mandatory, not discretionary. Compl. ¶¶

82, 98, 180. From 2007 through 2015, the IG warned OPM each year that it remained out of compliance with binding data security standards of the Federal Information Security Management Act, 44 U.S.C. § 3541, *et seq.*, superseded by the Federal Information Modernization Act of 2014 (collectively, "FISMA"). Compl. ¶¶ 81–113, 180, 198–200.

OPM's conduct "must be viewed in [its] context." *Waters*, 888 F.2d at 876. The IG found for several consecutive years that OPM's data security policies, practices, and governance suffered from "material weaknesses" in violation of FISMA, presenting an immediate risk to the security of assets or operations. Compl. ¶¶ 87–88. In 2010 the IG determined that OPM's process for certifying and accrediting (*i.e.*, authorizing) system security controls was rife with deficiencies. *Id*. ¶ 100. OPM allowed the situation to deteriorate. In 2014 the IG found no assurance that security controls were in place at OPM, concluding the agency still had no way to monitor its information systems. *Id*. ¶ 103. The IG informed OPM that over half of its systems—including some of its "most critical and sensitive applications"—were at risk and that these weaknesses "raised national security implications." *Id.* ¶ 102. The IG took the unprecedented step of advising OPM to shut down these vulnerable systems; but OPM ignored the advice and refused to take action to protect Plaintiffs' data. *Id*. ¶¶ 103–04.

At the same time the IG was warning OPM of the material deficiencies in its information systems, OPM was aware that unauthorized persons were continually attempting to breach those systems and had, on occasion, succeeded in doing so. The complaint alleges that OPM was aware of breaches of other federal agencies' systems and the fact that every month saw "at least 10 million" attempted intrusions into OPM's own systems. Compl. ¶¶ 79–80. The agency publicly disclosed actual breaches in 2009 and 2012. *Id.* ¶ 78. In 2014, OPM learned that the information systems of two companies it had enlisted to conduct personnel investigations,

including Defendant KeyPoint's systems, had suffered data breaches. *Id.* ¶¶ 114–18.

These allegations confirm that OPM knew that its data security was woefully inadequate and noncompliant with federal law and that data thieves were making every effort to exploit those deficiencies. In short, the question was not "if," but "when." OPM failed to obey federal law and adopt reasonable security measures. Taken as a whole, Plaintiffs' allegations provide a "logical basis" to conclude that OPM made a willful or intentional decision to violate federal law. *Cf.* OPM Mot. at 45.

A number of courts have found similar or less reckless conduct sufficient to satisfy the Privacy Act's "intentional and willful" standard. In *Schmidt v. U.S. Department of Veteran Affairs*, for example, the court found that evidence of the agency's failure to install electronic security patches established its "intentional" or "willful" noncompliance with section 552a(e)(10) and that plaintiffs were entitled to statutory damages because the agency's failure to do so evinced "a complete disregard for the security and confidentiality of" Social Security numbers and "a complete lack of anticipation of the potential for abuse." 218 F.R.D. 619, 634–36 (E.D. Wis. 2003), *dismissed on other grounds*, 222 F.R.D. 592 (E.D. Wis. 2004); *compare* Compl. ¶¶ 107, 135 ("In multiple FISMA audits, the IG found that OPM was not adequately patching its software systems and that its failure to do so represented an information security deficiency."). In *VA Data Theft*, allegations that the agency had been "warned repeatedly of deficiencies in [its] information security and yet failed to do anything to establish proper safeguards," sufficed to plead the agency "acted with something greater than gross negligence." 2007 WL 7621261, at *4; *see also Makowski v. United States*, 27 F. Supp. 3d 901, 913–14 (N.D. Ill. 2014) (finding that allegations that a federal agency failed to update records, in spite of being notified of inaccuracies and potential for adverse consequences, sufficed to plead flagrant

disregard under the Privacy Act); *Feldman v. CIA*, 797 F. Supp. 2d 29, 42 (D.D.C. 2011) ("Viewing the plaintiff's allegations in the light most favorable to the plaintiff . . . the Court finds that the totality of the plaintiff's allegations do adequately allege intentional or willful conduct."); *Tolbert-Smith v. Chu*, 714 F. Supp. 2d 37, 43 (D.D.C. 2010); *Hawley*, 543 F. Supp. 2d at 51–52 (complaint pled "intentional" or "willful" as it alleged agency was "repeatedly informed of recurring, systemic, and fundamental deficiencies in its information security").

Here, the complaint's allegations of warnings and admonitions, potential for harm, and knowledge of actual attempted intrusions are at least as extensive as those held sufficient in *Schmidt*, *VA Data Theft*, *Makowski*, and *Hawley*. OPM was warned about its alarming data security by its own IG, which has a statutory mandate of advising OPM of its noncompliance with federal law. There was not just one warning—OPM received repeated and detailed warnings over the course of eight years. OPM officials knew, moreover, that failing to cure these deficiencies placed the sensitive personal information of every federal employee at risk. As noted, prior to the Data Breaches, OPM's own systems had been breached on multiple occasions; OPM officials also knew that its contractors' and other federal agencies' systems had been breached and that several million attempted intrusions into OPM's systems were taking place each month. OPM's characterization of Plaintiffs' complaint as "completely devoid" of willfulness allegations is misplaced. OPM Mot. at 44. The facts as pled demonstrate OPM's reckless failure to safeguard Plaintiffs' records.

3. The Complaint Plausibly Alleges That OPM Willfully or Intentionally Violated the Nondisclosure Provision, Section 552a(b).

Plaintiffs' allegations of the unauthorized transmission of their records to hackers also state a claim for unauthorized disclosure under the Privacy Act. OPM notably recognizes, in its motion to dismiss the NTEU complaint for alleged constitutional violations, that the Act's

"comprehensive requirements give forceful recognition to a Government employee's interest in maintaining the confidentiality" of his or her personnel file, and that "while government accumulation of personal information for public purposes may pose a threat to privacy, these privacy concerns are generally allayed by a statutory or regulatory duty to avoid unwarranted disclosures." [Dkt. No. 81-1 at 19, 21 (quotation marks and citations omitted).] Even so, OPM challenges the class Plaintiffs' claim for wrongful disclosure under the Act, arguing that the final step that consummated the disclosure here—the theft by third-party wrongdoers—was beyond OPM's immediate control. OPM Mot. at 45. OPM's position, however, has been rejected by other courts under analogous circumstances and should be rejected in this case as well.

The *VA Data Theft* case was not analogous to this one. There, a VA employee took data home on a personal computer and an external hard drive. A burglar stole this equipment from his house. 2007 WL 7621261, at *1. The court found that allegations that the GAO had warned the agency of its systemic security weaknesses stated a claim that the agency intentionally or willfully failed to comply with the safeguards provision of the Privacy Act. *Id*. at *4–5. At the same time, the court dismissed the claim under the nondisclosure provision as the stealing of the laptop did not constitute a transmission or disclosure of information and both the agency's IG and the FBI were "highly confident" that there had subsequently been no unauthorized transmission of the plaintiffs' information. *Id*. at *1, *5–6.

The facts before the Court more closely resemble those in *Beaven v. United States Department of Justice*, 622 F.3d 540 (6th Cir. 2010). In *Beaven*, a federal investigator left an unmarked file folder that contained personal information about prison employees in a prison's common area. *Id.* at 544–45. The evidence suggested that one inmate viewed the contents of the folder. *Id*. at 545. That the folder was not marked with any warnings made it more likely that

someone would look at it. *Id.* at 552–53. The court affirmed a finding that the agent's "*course of conduct* resulted in a disclosure . . . and that his actions were 'intentional or willful' . . . although his *final act* of leaving the folder unsecured was 'inadvertent.'" *Id.* at 547 (emphasis in original). As the Court of Appeals explained, "a court may consider the entire course of conduct that resulted in the disclosure in making its required finding under § 552a(g)(4). Such an interpretation will allow recovery under circumstances similar to those here, where an agency's actions, although inadvertent at the last step, were in flagrant disregard of the plaintiff's rights under the Privacy Act at other steps along the way." *Id.* at 551. Similarly, in *Tolbert-Smith*, another case OPM neglects to cite, a court in this District upheld a Privacy Act claim for unlawful disclosure based on allegations that data had been willfully or intentionally left on a server that was accessible to third parties. 714 F. Supp. 2d at 43.

Plaintiffs' allegations, therefore, render *VA Data Theft* inapposite and bring this case squarely under *Beaven* and *Tolbert-Smith*. Just as the investigator's act of leaving an unmarked file folder in a prison common area created a substantial risk of disclosure in *Beaven*, so OPM's leaving Plaintiffs' sensitive personal information exposed on servers that were vulnerable and subject to regular attack created a substantial risk of disclosure here. Yet, while in *Beaven* the information was exposed inadvertently, OPM officials actually knew that disclosure of Plaintiffs' information was likely. Compl. ¶¶ 2–3, 179. OPM officials nevertheless chose to leave the information on an unsecured server. The only significant distinction between *Beaven* and this case is that the risk OPM ignored was not vague, but a virtual certainty.

III. THE COMPLAINT STATES A CLAIM UNDER THE ADMINISTRATIVE PROCEDURE ACT.

Plaintiffs seek declaratory and injunctive relief under the Administrative Procedure Act ("APA") to address OPM's recalcitrant failure to implement a data security plan that satisfies the

requirements of FISMA and federal standards. Compl. ¶¶ 196–207. The APA requires courts to compel agency action unlawfully withheld or unreasonably delayed. 5 U.S.C. § 706(1). It also requires courts to hold unlawful and set aside agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Id.* § 706(2)(A). Plaintiffs allege that OPM has unlawfully withheld and unreasonably delayed actions mandated by law and acted in a manner that is arbitrary, capricious, and not in accordance with law. As shown below, Plaintiffs state a claim for relief under the APA.

A. The Privacy Act Does Not Preclude Plaintiffs from Seeking Equitable Relief Under the Administrative Procedure Act.

The APA authorizes judicial review of agency action whenever "there is no other adequate remedy in a court." 5 U.S.C. § 704. Because the Privacy Act does not permit a court to set aside actions that are arbitrary, capricious, or an abuse of discretion; does not provide equitable relief for the violations alleged here; and does not otherwise provide relief that would prevent the ongoing and future injury to Plaintiffs' statutory rights, Plaintiffs have no "adequate remedy in a court" other than the remedy the APA provides.

The D.C. Circuit has rejected OPM's argument that Congress intended to preclude relief under the APA for conduct that also violates the Privacy Act. The D.C. Circuit has long recognized, instead, that a court may enjoin violations of the Privacy Act where the Privacy Act does not itself authorize such relief. A court may do so either by exercising its authority under the APA, *Doe v. Stephens*, 851 F.2d 1457, 1465–66 (D.C. Cir. 1988), or under its "inherent equitable powers," *Haase v. Sessions*, 893 F.2d 370, 374 n.6 (D.C. Cir. 1990).[8] The D.C.

[8] The court in *Haase* pointed out that, except for the provisions at 5 U.S.C. §§ 552a(g)(2) and (g)(3), the Privacy Act only provides monetary damages; the court reasoned in *dicta* that "[i]t is not at all clear to us that Congress intended to preclude broad equitable relief (injunctions) . . .

[Footnote continued on next page….]

Circuit, therefore, has not followed those decisions that have found that a court may award injunctive relief based on conduct that violates the Privacy Act only under the two scenarios specified in the Privacy Act. *See* OPM Mot. at 55 (citing, *inter alia*, *Cell Assocs., Inc. v. Nat'l Insts. of Health*, 579 F.2d 1155, 1161–62 (9th Cir. 1978); *Edison v. Dep't of the Army*, 672 F.2d 840, 846–47 (11th Cir. 1982); and *Parks v. IRS*, 618 F.2d 677, 683–84 (10th Cir. 1980)).

The D.C. Circuit holdings in this area accord with the Supreme Court's observation that Congress drafted the Privacy Act against the backdrop of the remedial provisions of the APA and the Court's recognition that the APA has supplied the predicate for Privacy Act enforcement.

> The Privacy Act says nothing about standards of proof governing equitable relief that may be open to victims of adverse determinations or effects, although it may be that this inattention is explained by the general provisions for equitable relief within the Administrative Procedure Act (APA), 5 U.S.C. § 706. Indeed, the District Court relied on the APA in determining that it had jurisdiction to enforce the stipulated order prohibiting the Department of Labor from using Social Security numbers in multiparty captions.

Chao, 540 U.S. at 619 n.1 (citing *Doe v. Herman*, No. 97-0043-B, 1998 WL 34194937, at *5–7 (W.D. Va. Mar. 18, 1998)).

Following *Chao*, a court in this District held that it retained authority under the APA to grant injunctive and declaratory relief to redress violations of the Privacy Act for which the Privacy Act itself provided no equitable remedies. *Radack v. U.S. Dept. of Justice*, 402 F. Supp. 2d 99, 104 (D.D.C. 2005). The court rejected the argument that, by authorizing only damages for certain Privacy Act violations, Congress had made damages the exclusive remedy for such conduct. *Id.* As a result, the court allowed an APA claim for equitable relief to proceed

---

[a]nd in the absence of such an explicit intention, by creating a general cause of action (under (g)(1)(D)) for violations of the Privacy Act, Congress presumably intended the district court to use its inherent equitable powers . . . ." 893 F.2d at 374 n.6.

alongside a parallel Privacy Act claim for damages. *Id*. The court explained, first, that "[b]ecause [plaintiff] seeks declaratory and injunctive relief in addition to damages, the Privacy Act does not provide an 'adequate remedy'" under 5 U.S.C. § 704, and, second, that the alleged Privacy Act violation concerned the unlawful release of information whereas the APA claim centered primarily upon the agency's failure to follow its internal policies. *Radack*, 402 F. Supp. 2d at 104. Under *Chao* and *Radack*, Plaintiffs may maintain their APA claim together with their Privacy Act claim.

The relief Plaintiffs seek under the APA is unavailable under the Privacy Act. Plaintiffs' APA claim seeks equitable relief to ensure that OPM brings its systems into compliance with federal statutes and standards. Compl. ¶¶ 196–215. Their Privacy Act claim, meanwhile, seeks damages for the injuries already caused by OPM's willful failure to safeguard, and unauthorized disclosure of, Plaintiffs' records. *Id.* ¶¶ 175–85. Plaintiffs' APA claim therefore seeks relief that is not of the "same genre" as that sought under the Privacy Act, *Odland v. FERC*, 34 F. Supp. 3d 3, 23 (D.D.C. 2014), and Plaintiffs have no adequate remedy under the Privacy Act that would afford them the relief they seek under the APA.

OPM's cases hold that a plaintiff may not seek the *same* relief under the Privacy Act and the APA.[9] *See* OPM Mot. at 55–56. As one reviewing court concluded, it is only when a

[9] *See Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) ("APA claim . . . is 'simply a restatement of . . . Privacy Act claims'") (citation omitted); *Wilson v. McHugh,* 842 F. Supp. 2d 310, 320 (D.D.C. 2012) ("To the extent he relies on the Privacy Act and believes the Privacy Act provides him a legal remedy . . . Wilson cannot seek review in this Court under the APA.") *Doe P v. Goss*, No. 04-2122, 2007 WL 106523, at *6 n.8 (D.D.C. Jan. 12, 2007) (plaintiff could not "pursue . . . claim pursuant to the APA" when Privacy Act also "provide[d] for . . . review"); *El Badrawi v. DHS*, 579 F. Supp. 2d 249, 280 n.35 (D. Conn. 2008) (plaintiff could not seek amendment of personnel records under APA because Privacy Act creates cause of action to amend personnel records and Congress has explicitly limited right to such relief to U.S. citizens); *Reid v. Fed. Bureau of Prisons*, No. 04-1845, 2005 WL 1699425, at *2 (D.D.C. July 20, 2005)

[Footnote continued on next page….]

plaintiff seeks identical relief for a violation of a statute under both the APA and the statute itself that the APA claim becomes invalid:

> [Plaintiff's] requested relief under both FOIA and the APA distinguishes this case from *Radack*. There, the claimant had requested monetary relief under the Privacy Act and declaratory and injunctive relief under the APA. Here, by contrast, [plaintiff] seeks declaratory judgment and a court order requiring the production of documents under both its APA claim and its FOIA claim. FOIA therefore provides [plaintiff] with an "adequate remedy in a court."

Central Platte Nat. Res. Dist. v. U.S. Dept. of Agric., 643 F.3d 1142, 1149 (8th Cir. 2011) (citations omitted). In short, OPM's authorities found that APA claims were "simply a restatement of . . . Privacy Act claims" and, thus, that the Privacy Act afforded a complete and adequate remedy. *Westcott*, 39 F. Supp. 3d at 33 (citation omitted).

Plaintiffs' APA claim neither restates nor reframes their Privacy Act claim, but provides independent legal grounds for prospective relief. For example, Plaintiffs allege that OPM has violated the APA by failing to comply with FISMA and the technical standards for data security issued by the Office of Management and Budget ("OMB") and the National Institute for Standards and Technology ("NIST") that bind OPM. Compl. ¶¶ 198–206. An "agency's failure

---

(dismissing APA claim seeking amendment of records because Privacy Act provided adequate remedy); *Ware v. U.S. Dep't of Interior*, No. 05-3033, 2006 WL 1005091, at *3 (D. Or. Apr. 14, 2006) (same); *Arruda & Beaudoin, LLP v. Astrue*, No. 11-10254, 2013 WL 1309249, at *15 (D. Mass. Mar. 27, 2013) (dismissing APA claim as "the APA provides no relief to the Plaintiffs other than that which is provided by the Privacy Act"); *Mittleman v. King*, No. 93-1869, 1997 WL 911801, at *4 (D.D.C. 1997) (dismissing APA claims to the extent they sought relief available under the Privacy Act and requesting supplemental briefing to the extent they did not); *Mittleman v. U.S. Treasury*, 773 F. Supp. 442, 449 (D.D.C. 1991) ("[P]laintiff's APA claim is, in part, simply a restatement of her Privacy Act claims"); *Schaeuble v. Reno*, 87 F. Supp. 2d 383, 393–94 (D.N.J. 2000) (dismissing APA claim as "identical to . . . Privacy Act claim") (citing *Mittleman*, 773 F. Supp. at 449). The one case arguably to the contrary, *Diaz-Bernal v. Myers*, did not concern the Privacy Act, and in the case addressing the Privacy Act that it cited, the plaintiff's complaint invoked neither the Privacy Act nor the APA. 758 F. Supp. 2d 106, 119 (D. Conn. 2010) (citing *El Badrawi*, 579 F. Supp. 2d at 280 n.35).

to follow its own regulations can be challenged under the APA," *Webster v. Doe*, 486 U.S. 592, 602 n.7 (1988), but cannot be challenged under the Privacy Act. Plaintiffs relatedly seek equitable relief to require OPM to perform actions it is legally required to perform but has unreasonably delayed and unlawfully withheld. Compl. ¶¶ 197, 207–15. This states a cause of action under the APA, but, again, *not* under the Privacy Act.

Thus, in addition to seeking remedies uniquely available under the APA, Plaintiffs bring APA claims that simply are not cognizable under the Privacy Act. The Privacy Act does not provide an "adequate remedy" under section 704 and these APA claims are not foreclosed.

B. The APA Requires the Court to Compel OPM to Perform Actions Mandated by Law That Have Been Unlawfully Withheld or Unreasonably Delayed.

The APA subjects to judicial review "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. Ordinarily, an agency action is considered final and reviewable if it (1) "mark[s] the consummation of the agency's decisionmaking process," and (2) determines "rights or obligations" or produces "legal consequences." *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997) (quotation marks and citations omitted). However, the APA also imposes a duty upon federal agencies to take required actions "within a reasonable time." *Fort Sill Apache Tribe v. National Indian Gaming Comm'n*, 103 F. Supp. 3d 113, 119 (D.D.C. 2015) (citing *Mashpee Wampanoag Tribal Council, Inc. v. Norton*, 336 F.3d 1094, 1099–1100 (D.C. Cir. 2003)). Therefore, the scope of judicial review under the APA extends to actions that have been "unlawfully withheld or unreasonably delayed," 5 U.S.C. § 706(1), such that a court must "compel agency action" when the agency has failed to take a discrete and required action within a reasonable time pursuant to a non-discretionary duty. *Norton v. Southern Utah Wilderness Alliance*, 542 U.S. 55, 62–64 (2004).

1. OPM's Compliance with the Federal Information Security Management Act and with Federal Data Security Standards Is Not Committed to Agency Discretion by Law.

FISMA mandates that "[t]he head of each agency *shall* . . . be responsible for . . . providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" information collected by that agency and maintained on its computer systems and those of its contractors, 44 U.S.C. § 3554(a)(1)(A) (emphasis added), as well as for "complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including," among other sources of law, standards promulgated by the National Institute for Standards and Technology, *id.* § 3544(a)(1)(B). Plaintiffs allege that OPM has persistently failed to perform its duties under FISMA, and ask this Court to enjoin OPM under the APA to perform those actions it has unreasonably delayed or unlawfully withheld.

OPM objects that FISMA represents one of "those rare instances" where a statute is "drawn in such broad terms that in a given case there is no law to apply" and that its compliance with FISMA is a matter "committed to agency discretion by law." OPM Mot. at 57 (citing *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971). But a review of FISMA and the standards it imposes on OPM dispels any notion of this being a rare case in which there is no law to apply.

Section 3554 of FISMA mandates that the Director of OPM "*shall*" "provide," "comply," "ensure," "determine," "develop," "implement," and "evaluate" security measures. 44 U.S.C. § 3554(a) (emphasis added). The Act requires agency heads and officials to continuously monitor and assess security controls and risks. *Id*. The agency head must also appoint and delegate certain responsibilities to a Chief Information Officer. *Id.* §§ 3554(a)(3), 3506(a)(2)(A). The

Act requires agencies to "develop, document, and implement an agency-wide information security program" including "policies and procedures" that will "*ensure compliance* with—(i) the *requirements* of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration *requirements*, as determined by the agency; and (iv) any other applicable *requirements* . . . ." *Id.* § 3554(b)(2)(D)(i)–(iv) (emphases added). The Act requires agencies to conduct "periodic testing and evaluation" of their "information security policies, procedures, and practices . . . no less than annually," including compulsory testing of "of every information system identified in the inventory required under section 3505(c)." *Id.* § 3554(b)(5). Section 3505(c) provides that the "head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency." *Id.* § 3505(c). The Act also requires that each agency "ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines," and ensure that agency personnel and contractors are adequately trained to detect, report on, and respond to security incidents. *Id.* §§ 3554(a)(4), (a)(7). Accordingly, FISMA is not a statute that permits OPM to take whatever action it deems to be in the interests of justice or in furtherance of data security. FISMA instead *requires* OPM to take *definite* steps and to comply with specific standards to protect the records in its care.

In addition to FISMA noncompliance, the complaint alleges (¶ 106), and the IG found in its 2014 Audit Report,[10] that OPM failed to implement the multi-factor authentication required

[10] U.S. Office of Personnel Management, Office of the Inspector General, Final Audit Report: Federal Information Security Management Act Audit FY 2014 at 24 (Nov. 12, 2014) ("IG 2014

[Footnote continued on next page….]

by Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11. The directive states that "[a]s promptly as possible, but in no case later than 8 months after the date of promulgation," the heads of executive departments and agencies "shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining . . . access to Federally controlled information systems." Homeland Security Presidential Directive 12, ¶ 4.[11] The President issued this directive nearly a dozen years ago, on August 27, 2004. OMB Memorandum M-11-11 builds on the directive:

> Effective immediately, all new systems under development ***must*** be enabled to use PIV [Federal Personal Identity Verification (PIV) smartcard] credentials, in accordance with NIST guidelines, prior to being made operational.
>
> Effective the beginning of FY2012, existing physical and logical access control systems ***must*** be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.

OMB Memorandum M-11-11 at 3–4.[12] That almost twelve years have passed without OPM complying with these mandatory standards, and the personnel information of almost every federal employee has been compromised, constitutes agency action unreasonably delayed.

OPM also has failed to implement in a timely manner the standards for personal identification verification credentials set forth in the National Institute for Standards and

---

Audit"), *available at* https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[11] Department of Homeland Security, Homeland Security Presidential Directive 12 (Aug. 27, 2004) (click on "HSPD 12 Full Text"), *available at* https://www.dhs.gov/homeland-security-presidential-directive-12.

[12] Memorandum from Jacob J. Lew, Dir., Executive Office of the President, on Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 (Feb. 3, 2011) (emphasis added), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.

Technology's Federal Information Processing Standards Publication 201-2.[13] Section 4.2 of this publication sets out the "mandatory data elements [that] are part of the data model for" these credentials, *i.e.*, the different levels of verification required to access information systems. Section 6.3.2 details the minimum requirements for access. Even at the lowest level of confidence, "Cardholder Unique Identifier" status is mandated to access government information systems. Yet as of the end of fiscal year 2014, "none of [OPM's] 47 major applications require[d] [personal identification verification] authentication." IG 2014 Audit at 24; *accord* Compl. ¶ 106.

Courts have construed and enforced agency compliance with standards far less concrete than the above data security standards. For example, in *Cody v. Cox*, the court found that the phrase "high quality and cost-effective health care" was sufficiently definite so as not to commit the matter to agency discretion, permitting judicial review. 509 F.3d 606, 610 (D.C. Cir. 2007) ("We have regularly found Congress has not committed decisions to agency discretion under far more permissive and indeterminate language."). In like vein, the court in *Dickson v. Secretary of Defense* found that a provision that a board "may" take an action if it "finds it to be in the interest of justice" constituted a "meaningful standard against which to judge the agency's exercise of discretion." 68 F.3d 1396, 1399–04 (D.C. Cir. 1995). Considered against these precedents, the statutory requirements promulgated by and under the Federal Information Security Management Act are sufficiently concrete to permit judicial review of OPM's failure to perform its duties under this Act.

[13] Department of Commerce, Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug. 2013), *available at* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

It bears emphasis that these requirements are mandatory. As stated in the IG's 2014 Audit Report, "of the 21 OPM systems due for Authorization in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization" even though "OMB Circular A-130, Appendix III *mandates* that all Federal information systems have a valid Authorization."[14] While OPM states that "'adequate security' is a flexible concept" as defined in this OMB circular (OPM Mot. at 62), what OPM neglects to mention is that "authorization" is not—"agency programs *shall* include the following controls in their general support systems and major applications . . . written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems." OMB Circular A-130, App'x III, at A.3.a.(2)(g)[15]; *see also id.* at B.a.(4) (providing that authorization must be granted by management and "is not a decision that should be made by the security staff").

OPM's broad noncompliance is not only longstanding, but ongoing.

- As of November 2015, "none of OPM's major applications required multi-factor authentication as required by OMB Memorandum M-11-11." Compl. ¶ 156.
- "The IG's November 2015 FISMA audit concluded that a lack of compliance 'seems to permeate' OPM's information security regime and that 'OPM continues to fail to meet FISMA requirements.'" *Id*. ¶ 152.
- The IG stated in November 2015 that "it was 'very concerned' about another attack occurring and that OPM's conscious decision not to ensure valid authorizations for its systems was 'irresponsible,' and an 'extremely poor decision.'" *Id.* ¶ 153.

Finally, OPM is wrong to imply that Plaintiffs challenge particular "choices" OPM made concerning "its FISMA obligations[.]" OPM Mot. at 58. Plaintiffs challenge OPM's overall,

[14] IG 2014 Audit at 9–10.

[15] Office of Management and Budget, Appendix III to OMB Circular No. A-130 (emphasis added), *available at* https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

persistent, and flagrant disregard for its statutory duties and a set of discrete regulatory directives. Although a federal agency enjoys discretion in determining precisely *how* to meet requirements, it has no discretion in determining *whether* to meet them. *See, e.g.*, *St. Christopher Assocs., L.P. v. United States*, 75 Fed. Cl. 1, 11 (2006) ("The Complaint . . . does not allege that the Government breached the contract by failing to approve the 1997 rent increase request, but rather by refusing to consider the request at all. A decision to consider a rent increase request, however, is not committed to agency discretion, and is therefore reviewable by this court."). Were this a case in which Plaintiffs were second-guessing the agency's choice of vendor or software program, OPM's argument might have some merit. But Plaintiffs do not challenge any one action that OPM *has* taken to protect Plaintiffs' privacy. Instead, Plaintiffs seek injunctive relief to redress the agency's persistent failure to take the required actions on the whole. The APA does not permit OPM to ignore the requirements of federal law with impunity.

In sum, Plaintiffs' APA claim seeks redress for OPM's continuing inaction, in the face of mandatory FISMA provisions and associated regulations, to protect Plaintiffs' sensitive personal information. The APA, 5 U.S.C. §§ 701–06, affords judicial review of this claim. 5 U.S.C. § 551(13); *Heckler v. Chaney*, 470 U.S. 821, 828 (1985).[16]

2. Plaintiffs Seek an Order Compelling OPM to Take Discrete Actions to Comply with Specific Legal Mandates.

OPM argues that the required actions it has failed to take are not "discrete" actions subject to APA review. *See* OPM Mot. at 64–66. In so arguing, OPM relies on *VA Data Theft* for the proposition that "the APA does not authorize courts to enter a general order compelling

[16] In a footnote, OPM recites actions and "reforms" that the government claims to be undertaking to address issues implicated in this litigation. *See* OPM Mot. at 66 n.37. This information falls outside the complaint and should be struck or, at a minimum, not considered on a motion to dismiss. *See* Fed. R. Civ. P. 12(d).

compliance with broad statutory mandates, especially in data breach cases like this one." OPM Mot. at 64 (citing *VA Data Theft*, 2007 WL 7621261, at *7). OPM's argument is unavailing.

The claims in *VA Data Theft* rested not on mandatory statutory provisions and regulations but exclusively on the minimum standards under the Privacy Act. 2007 WL 7621261, at *7. Plaintiffs here, by contrast, allege that OPM has failed (and continues to fail) to take numerous discrete actions in a reasonably timely manner that are independently required by binding law. For example, OPM operated multiple information systems without valid authorizations (Compl. ¶¶ 99–104) and failed to implement multi-factor authentication for systems access (*id*. ¶¶ 106, 137); *see also id.* ¶¶ 91–98, 113. Where "an agency is under an unequivocal statutory duty to act, failure so to act constitutes, in effect, an affirmative act that triggers 'final agency action' review." *Sierra Club v. Thomas*, 828 F.2d 783, 793 (D.C. Cir. 1987); *see also Public Citizen Health Research Grp. v. Commissioner, Food & Drug Admin.*, 740 F.2d 21, 32 (D.C. Cir. 1984). Indeed, "[w]ere it otherwise, agencies could effectively prevent judicial review of their policy determinations by simply refusing to take final action." *Cobell v. Norton*, 240 F.3d 1081, 1095 (D.C. Cir. 2001). OPM was under an unequivocal statutory duty here and its failure to timely comply is reviewable under 5 U.S.C. § 706.

Again, Plaintiffs allege not only that OPM has failed to take specific and discrete actions it is required to take—although, to be sure, it has failed to do so—but also that OPM has failed to comply with FISMA and the Privacy Act on a wholesale level. The D.C. Circuit, when called on to review a wholesale failure by an agency to perform its fiduciary duties by keeping adequate records and by providing timely accounts to the beneficiaries of Individual Indian Money trusts, observed that in such a situation "delaying review is tantamount to denying review altogether." *Cobell*, 240 F.3d at 1095. Thus, the deference due to an agency that is attempting to perform its

duties under even a general statute "does not require courts to turn a blind eye when government officials fail to discharge their duties." *Id.* at 1096. That is what Plaintiffs allege happened here.

C. The Court May Appoint a Special Master to Oversee Technical Issues of Compliance.

OPM's argument suggests that to order injunctive relief here would be to enter a thicket of complex and technical oversight. Setting aside that many courts have supervised complex remedial programs at public institutions,[17] including federal agencies,[18] this Court has the option of appointing a special master to monitor OPM's discharge of its mandatory statutory duties. *See* Fed. R. Civ. P. 53. Appointment of a special master may be warranted in this case given two of its unique characteristics.

First, there is the recalcitrance exhibited by OPM, and described above, in complying with federal law and responding to the theft of Plaintiffs' data. *See, e.g.*, *Williams v. Lane*, 851 F.2d 867, 884 (7th Cir. 1988) (concluding that the appointment of a special master was appropriate because "[t]he record here is replete with instances of administrative recalcitrance."); *Hook v. Arizona*, 120 F.3d 921, 926 (9th Cir. 1997) (concluding that the appointment of a special master was appropriate because of the defendant's "history of noncompliance").

Second, appointment of a master with specialized expertise in data security would free this Court from the burdens of day-to-day involvement in monitoring OPM's efforts to carry out its duties under FISMA. *See Local 28 of Sheet Metal Workers' Int'l Assoc. v. EEOC*, 478 U.S. 421, 482 (1986) (finding that "in light of the difficulties inherent in monitoring compliance with

---

[17] *See, e.g.*, *Cordero v. Pennsylvania Dept. of Educ.*, 795 F. Supp. 1352, 1363–64 (M.D. Pa. 1992) (citing cases).

[18] *See, e.g.*, Note, *Judicial Control of Systemic Inadequacies in Federal Administrative Enforcement*, 88 Yale L.J. 407, 416–17 & nn.36–39 (1978) (citing D.D.C. cases).

the court's orders, and especially petitioners' established record of resistance to prior state and federal court orders designed to end their discriminatory membership practices, appointment of an administrator was well within the District Court's discretion."); *National Org. for the Reform of Marijuana Laws v. Mullen*, 828 F.2d 536, 542–43 (9th Cir. 1987) (affirming appointment of special master to monitor compliance with injunction against federal government entities, among others). Appointment of a special master may be warranted where a court determines that it lacks the practical means to monitor a defendant's efforts to bring itself into compliance. *See, e.g.*, *Hook*, 120 F.3d at 926; *Gary W. v. State of La.*, 601 F.2d 240, 244–45 (5th Cir. 1979) (finding that "the evidence of non-compliance with [the] final order and the need for daily supervision of the bureaucratic tangle . . . supports the District Court's conclusion.") (citing district court findings); *Halderman v. Pennhurst State Sch. & Hosp.*, 612 F.2d 84, 111 (3d Cir. 1979), *rev'd on other grounds*, 451 U.S. 1 (1981); *Salazar v. District of Columbia*, No. CA-93-452(GK), 1997 WL 306876, at *2 (D.D.C. 1997) (designating a monitor "given the need for both on-going monitoring requiring analysis of complex reports and studies as well as evaluation of new and costly enforcement mechanisms").

IV. THE COURT HAS THE INHERENT AUTHORITY TO ENTER EQUITABLE REMEDIES AGAINST OPM.

To the extent any of the equitable relief Plaintiffs request is not available under the APA, the Court may order that relief pursuant to its inherent authority. OPM erroneously claims that sovereign immunity bars the Court from entering such relief. *See* OPM Mot. at 67. As OPM concedes, Plaintiffs' complaint identifies the APA as a source for this Court's authority to enter relief against the government. *Id.*; Compl. ¶ 197. The APA provides that "[a]n action in a court of the United States seeking relief other than money damages and stating a claim that an agency . . . acted or failed to act in an official capacity or under color of legal authority shall not be

dismissed nor relief therein be denied on the ground that it is against the United States . . . ." 5 U.S.C. § 702. The D.C. Circuit has "expressly" and "repeatedly" held that this "waiver of sovereign immunity applies to *any* suit" seeking relief other than money damages, including nonstatutory review actions, "whether under the APA or not." *Trudeau v. FTC*, 456 F.3d 178, 186 (D.C. Cir. 2006) (emphasis added) (citations omitted); *accord DeBrew v. Atwood*, 792 F.3d 118, 124 (D.C. Cir. 2015). OPM argues that sovereign immunity nullifies this Court's authority to order equitable relief without acknowledging controlling decisions that reject this argument.

Acting under its inherent equitable powers, the Court may exercise discretion to order the equitable remedies of declaratory and injunctive relief when remedies at law are inadequate or unavailable. *See Mechling Barge Lines, Inc. v. United States*, 368 U.S. 324, 331 (1961) ("Declaratory judgment is a remedy committed to judicial discretion."); *Porter v. Warner Co.*, 328 U.S. 395, 398 (1946) ("Unless otherwise provided by statute, all the inherent equitable powers of the District Court are available for the proper and complete exercise of that jurisdiction."); *Pierce v. Society of Sisters of the Holy Names*, 268 U.S. 510, 536 (1925) ("Prevention of impending injury by unlawful action is a well-recognized function of courts of equity."). Injunctive relief is proper on a showing of irreparable harm and, in the context of the prior unlawful conduct of government officials, on a finding that such conduct likely will persist absent the injunction. *Wooley v. Maynard*, 430 U.S. 705, 712 (1977).

OPM's failure to protect the sensitive personal information of Plaintiffs and class members violated their privacy rights and resulted in concrete economic damage. OPM's failure to secure its information systems has been persistent and continues today. Compl. ¶¶ 81–113, 152–57. OPM's failure creates an imminent risk of harm to millions of class members. It is clearly harmful to the public interest. *Id.* ¶ 212. Under these extraordinary circumstances, an

injunction should be entered requiring OPM to bring its electronic security into compliance with federal law. *Id*. ¶ 215. And, at a minimum until OPM complies with such an injunction, OPM also should be required to indemnify class members who suffer identity theft or fraud in the future. *Id*. ¶ 213.[19]

V. NO IMMUNITY SHIELDS KEYPOINT GIVEN ITS ALLEGED VIOLATIONS.

KeyPoint's primary defense is that it should be afforded quasi-governmental immunity. *See* KP Mot. at 17–22. But in its recent decision in *Campbell-Ewald Co. v. Gomez*, the Supreme Court dismissed "the notion that private persons performing Government work acquire the Government's embracive immunity." 136 S. Ct. 663, 672 (2016). The Court held that "[w]hen a contractor violates both federal law and the Government's explicit instructions, as here alleged, no 'derivative immunity' shields the contractor from suit by persons adversely affected by the violation." *Id.* KeyPoint's plea for immunity should be dismissed under *Campbell-Ewald*.

Plaintiffs allege that KeyPoint violated section 552a(e)(10) of the Privacy Act "by failing to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to their security or integrity which could cause substantial harm,

[19] OPM claims that an injunction to provide identity theft protection and/or indemnification would amount to an award of money damages. *See* OPM Mot. at 67. OPM ignores the distinction the Supreme Court has long drawn under section 702 of the APA "between an action at law for damages—which are intended to provide a victim with monetary compensation for an injury to his person, property, or reputation—and an equitable action for specific relief—which may include an order providing for the reinstatement of an employee with backpay, or for the recovery of specific property or monies, ejectment from land, or injunction either directing or restraining the defendant officer's actions." *Bowen v. Massachusetts*, 487 U.S. 879, 893 (1988) (emphasis, quotation marks, and citation omitted). That the latter type of remedy "may require one party to pay money to another is not a sufficient reason to characterize the relief as 'money damages.'" *Id*. Thus, that the government would have to expend money in order to provide the protection required by the injunction requested here hardly converts it to a form of damages. This protection is intended, not to compensate Plaintiffs, but to secure the protection Congress intended for them and their personal information.

embarrassment, inconvenience, or unfairness to Plaintiffs and Class members." Compl. ¶ 123; *see also id*. ¶ 223 (detailing KeyPoint's data security violations). Plaintiffs also allege that KeyPoint violated section 552a(b) of the Privacy Act, "by disclosing Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose." Compl. ¶ 123. These allegations preclude derivative immunity.

KeyPoint argues for immunity under *Yearsley v. W.A. Ross Construction Co.*, 309 U.S. 18 (1940), without noting that the Supreme Court in *Campbell-Ewald* rejected a similar attempt to invoke *Yearsley* to avoid suit. Specifically, the Court distinguished *Yearsley* from "cases in which a Government agent had 'exceeded his authority'" such that "the agent could be held liable for conduct causing injury to another." 136 S. Ct. at 673 (citing *Yearsley*, 309 U.S. at 21). For "a key premise of *Yearsley*, and one that has been reiterated by [various federal courts] is that the contractor was following the sovereign's directives." *In re Fort Totten Metrorail Cases*, 895 F. Supp. 2d 48, 74 (D.D.C. 2012) (alteration in original) (citations omitted).

A contractor like KeyPoint that violates a federal statute has not followed the sovereign's directives. *See* Compl. ¶ 122 (alleging that "[b]y unreasonably failing to safeguard its security credentials and . . . GII [personally sensitive government investigation information], KeyPoint departed from its mandate" and "exceeded its authority"), ¶ 124 (alleging KeyPoint "depart[ed] from the commands and directives of federal law"). There is no private immunity for conduct the sovereign has forsworn and for which the sovereign has waived its own immunity. KeyPoint's immunity plea, moreover, is independently foreclosed on two other grounds.

First, the complaint alleges that, in failing to comply with the Privacy Act, KeyPoint breached the terms of its contract with OPM. Compl. ¶ 123; *see Campbell-Ewald*, 136 S. Ct. at 672 (holding that a federal contractor must obey the government's "explicit instructions" to be

covered by derivative sovereign immunity). Federal contracts necessarily incorporate the requirements of the Privacy Act. Compl. ¶ 123 (citing 5 U.S.C. § 552a(m)(1)). A contractor is not "following the sovereign's directive" when it breaches its contract with the government. *Fort Totten Metrorail Cases*, 895 F. Supp. 2d at 74. Therefore, no immunity applies.

Second, KeyPoint acted negligently, by, among other things, failing to secure its computers and software, encrypt Plaintiffs' data, and monitor its data systems. Compl. ¶¶ 124, 223. "[D]erivative sovereign immunity is not available to contractors who act negligently in performing their obligations under the contract." *Fort Totten Metrorail Cases*, 895 F. Supp. 2d at 74; *see also City of Worcester v. HCA Mgmt. Co.*, 753 F. Supp. 31, 38 (D. Mass. 1990) (holding that derivative immunity does not apply "when a private corporation who performs governmental duties pursuant to contractual authority from the government is sued for negligence in the performance of these duties.").

VI. THE TORT CAUSES OF ACTION AGAINST KEYPOINT ARE WELL-PLED.

A. The Laws of the States in Which Plaintiffs Were Injured Govern Their Common-Law Claims.

In a footnote, KeyPoint argues that D.C. law should govern all the common-law claims. *See* KP Mot. at 35 n.30. Yet KeyPoint's own choice-of-law authority recognizes the site of the injury as the primary factor for determining governing law. *Id*. (citing, *inter alia*, Restatement (Second) of Conflict of Laws § 145). Plaintiffs sustained injury in their home states. The laws of those states accordingly govern their claims at common law.

Plaintiffs agree that the threshold choice-of-law rules of the District of Columbia govern the choice-of-law analysis here. In determining which jurisdiction has the most significant relationship to a dispute, D.C. courts consider the four Restatement factors: "(1) 'the place where the injury occurred'; (2) 'the place where the conduct causing the injury occurred'; (3) 'the

domicil, residence, nationality, place of incorporation and place of business of the parties'; and (4) 'the place where the relationship, if any, between the parties is centered.'" *Estate of Botvin ex rel. Ellis v. Islamic Republic of Iran*, 684 F. Supp. 2d 34, 39 (D.D.C. 2010) (citation omitted).

The first Restatement factor—the place of injury—normally controls the choice-of-law analysis in tort actions. *RDO Foods Co. v. United Brands Int'l, Inc*., 194 F. Supp. 2d 962, 976 (D.N.D. 2002) ("The most important of these contacts is the place where the injury occurred."); *Hager v. Crepaco, Inc*., 980 F. Supp. 292, 294 (N.D. Ill. 1997) ("[T]he place where the injury occurred, is considered the most important factor in this analysis."). Courts in this District apply this principle and it applies here. *See, e.g*., *Hourani v. Psybersolutions LLC*, No. 15-CV-933 (RMC), 2016 WL 659669, at *7 (D.D.C. Feb. 18, 2016) ("Any injury [plaintiff] may have suffered due to the alleged torts occurred in Virginia, where he lives. Accordingly, Virginia law applies."); *Brannen v. Nat'l R.R. Passenger Corp*., 403 F. Supp. 2d 89, 95 n.2 (D.D.C. 2005) ("Because Maryland is the place where the injury occurred and where the conduct causing the injury occurred, Maryland law applies to the plaintiff's negligence claims.").

KeyPoint maintains that D.C. law should govern Plaintiffs' claims against it on the basis that "Plaintiffs' claims are centered around D.C." KP Mot. at 35 n.30. But, in fact, KeyPoint is headquartered with its principal place of business in Loveland, Colorado, while Plaintiffs reside in 24 states across the country. Compl. ¶¶ 10–50, 53. It is in those states that Plaintiffs were injured. *Id.* ¶¶ 13–50; *see Target*, 66 F. Supp. 3d at 1171–77 (analyzing negligence claims arising from the breach of Target's electronic systems under the respective laws of each plaintiff's home state). Further, the conduct that was a cause of Plaintiffs' injuries occurred in the state in which KeyPoint's negligent security practices originated—Colorado. Even assuming KeyPoint's business dealings with OPM were centered in D.C., nothing in the complaint

suggests that any of KeyPoint's unlawful conduct occurred in D.C., and most of the Plaintiffs neither live nor work (nor transact business) in D.C. Compl. ¶¶ 13–50. Given these circumstances, D.C. law does not govern Plaintiffs' common-law claims.

B. The Complaint States a Claim for Negligence.

1. Plaintiffs Adequately Allege a Duty of Care.

The elements of negligence are (1) duty, (2) breach, (3) causation, and (4) damages. *Fisher v. Delta Airlines*, No. 3:09-CV-567-HEH, 2009 WL 3193151, at *1 n.1 (E.D. Va. Oct. 5, 2009) (citing 57A Am. Jur. 2d Negligence § 71). Plaintiffs allege KeyPoint owed them a duty of care to protect their personal information, and the KeyPoint log-in credentials that are used to access that information on KeyPoint's and OPM's systems, "through security procedures, protocols, and systems that are reasonable, adequate, and in conformance with recognized data security industry standards." Compl. ¶ 218(d).

KeyPoint cannot seriously deny its duty to establish reasonable safeguards to protect the information it collected. The Fair Credit Reporting Act ("FCRA") requires KeyPoint to "maintain reasonable procedures" to protect this information. 15 U.S.C. § 1681e(a); Compl. ¶¶ 246, 250. FISMA, whose predominant purpose is to ensure data security, also imposes a duty of care on KeyPoint. 44 U.S.C. §§ 3551, 3554(a) & (b). This duty is co-extensive with that imposed by state laws. *See, e.g.*, Cal. Civ. Code § 1798.81.5(b) ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access . . . or disclosure.").[20]

[20] *See also, e.g.*, N.C. Gen. Stat. Ann. § 75-64(a) (providing that "any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable

[Footnote continued on next page….]

KeyPoint nonetheless disputes the existence of this duty, claiming that it could not have foreseen that "criminals—perhaps working in connection with a foreign sovereign" would seek to breach its systems. KP Mot. at 36–37. Speculation aside, KeyPoint cannot credibly maintain that these data breaches were not foreseeable when its own argument (albeit one based on material outside the complaint) is that such incidents are "commonplace," and often successful. KP Mot. at 15–16, 38. The duty to take care to protect Plaintiffs' information existed, not only pursuant to statute, but because the cyberattacks were a reasonably foreseeable consequence of KeyPoint's misconduct, their criminal nature notwithstanding.

a. KeyPoint Had a Duty Not to Subject Plaintiffs to an Unreasonable Risk of Harm.

A duty to exercise reasonable care arises when an actor's conduct produces a risk of harm to another person. This is the "ordinary tort duty that every person owes not to impose foreseeable harm on others by negligent acts." *In re Davis*, 172 B.R. 437, 456 (Bankr. D.D.C. 1994); *see also FGA, Inc. v. Giglio*, 278 P.3d 490, 501 (Nev. 2012) (reiterating "duty of all persons to 'exercise reasonable care not to subject others to an unreasonable risk of harm.'") (citations omitted). It follows that "[i]n the ordinary case . . . the defendant does owe a duty of care." Dan B. Dobbs et al., The Law of Torts § 125 (2d ed.).

---

measures to protect against unauthorized access to or use of the information in connection with or after its disposal."); Nev. Rev. Stat. Ann. § 603A.210(1) ("A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."); Utah Code Ann. § 13-44-201(1)(a) ("Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to . . . prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business.").

KeyPoint is not relieved of duty because wrongful acts were committed by third parties. *See In re The Home Depot, Inc., Customer Data Security Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."); *In re Target Corp. Customer Data Security Breach Litig.*, 64 F. Supp. 3d 1304, 1308 (D. Minn. 2014) ("[G]eneral negligence law imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff.") (citations omitted). Plaintiffs here plausibly allege that KeyPoint's unreasonable failure to safeguard their information created a foreseeable risk of harm to them. Compl. ¶¶ 217, 223.

KeyPoint mistakenly argues that Plaintiffs' common-law negligence claims (and several other of their claims) lack merit on the grounds that the complaint does not itemize whose information was compromised by KeyPoint and whose by OPM. *See* KP Mot. at 37. KeyPoint's argument fails for the same reason it fails to defeat Plaintiffs' standing: a complaint need not plead which defendant breached a duty to which plaintiff when that information is in the defendants' exclusive possession. *See supra* Section I.A.2.a & fn. 6; *see also Neiman Marcus*, 794 F.3d at 696 ("If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury.'") (citing *Price Waterhouse*, 490 U.S. at 263) (O'Connor, J., concurring in the judgment) (citing *Summers*, 199 P.2d at 3–4)). It therefore suffices that Plaintiffs allege KeyPoint breached not only its duty to the 48,000 class members whose information it directly disclosed (Compl. ¶

120) but also its general duty of care to all of the class members, whose information it foreseeably put at risk with its inadequate data security (*id*. ¶¶ 217–23).

b. KeyPoint Had a Duty to Guard Against a Foreseeable Criminal Data Breach.

KeyPoint's claim that it had no "ordinary" duty to defend against intervening criminal acts fares no better because the Data Breaches against which KeyPoint failed to defend were entirely foreseeable. KP Mot. at 36. Although a random and unforeseeable criminal act may break the causal chain under certain circumstances, there are "some criminal acts [that] may be a reasonably foreseeable consequence of circumstances created by the defendant." *Mays v. City of Middletown*, 70 A.D.3d 900, 902 (N.Y. App. Div. 2010) (quotation marks and citations omitted). And when "a criminal or intentional intervening act is foreseeable, or is part of the original risk negligently created by the defendant in the first place, then the harm is not outside the scope of the defendant's liability." Dan B. Dobbs et al., The Law of Torts § 209 (2d ed.). Thus, an actor remains liable if his negligence enabled a crime and "the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime." Restatement (Second) of Torts § 448. Here, because a criminal data theft was a reasonably foreseeable consequence of deficient data security (Compl. ¶¶ 76, 217, 223), KeyPoint had a duty to implement effective data security to protect against it.

Even in jurisdictions like the District of Columbia that call for a heightened showing of foreseeability when there has been an intervening criminal act, "[i]f the danger of an intervening negligent or criminal act should have reasonably been anticipated and protected against, the defendant will be held responsible for the damages which result despite the entry of another act in the chain of causation." *Piedmont Resolution, L.L.C. v. Johnston*, *Rivlin & Foley*, 999 F.

Supp. 34, 58 (D.D.C. 1998). In particular, "the requirement [of a heightened showing of foreseeability] can be met . . . by a combination of factors which give the defendant an increased awareness of the danger of a particular criminal act," and "[i]f the relationship between the parties strongly suggests a duty of protection, then specific evidence of foreseeability is less important." *Smith v. Hope Vill., Inc.*, 481 F. Supp. 2d 172, 189 (D.D.C. 2007) (alterations in original) (citation omitted).

Plaintiffs' allegations satisfy even this heightened standard. KeyPoint was well aware of the danger given both the sensitivity of the information at its disposal and the nature of the investigatory services it performed. KeyPoint's increased awareness of the danger of data theft resulted in part from the fact that it was gathering and storing highly sensitive information for OPM—known to be a "prime target for cyberattacks." Compl. ¶ 3. Furthermore, KeyPoint was specifically aware that a breach of its systems would expose all of OPM's systems because these systems were linked in order to facilitate the sharing of information. *Id*. ¶ 217. As the complaint explains, an electronic conduit known as the "Secure Portal" connected the two entities' networks, allowing KeyPoint investigators to download forms and other information from OPM and to upload their investigatory findings back onto OPM's servers. *Id*. ¶ 76.

KeyPoint disputes none of these facts and fails to note that Plaintiffs do, in fact, allege a "special relationship" with KeyPoint by virtue of the unique information they provided. *Compare* KP Mot. at 36, *with* Compl. ¶ 221. KeyPoint instead asserts, without support, that it was "completely separate" from OPM and could not have anticipated that an attack on its network would also expose data on OPM's servers. KP Mot. at 36–37 (emphasis omitted). KeyPoint's bare assertions defy common sense and contradict the allegations of the complaint. The very purpose of KeyPoint's engagement was to conduct background investigations on behalf

of OPM. As a result, it was inevitable that information collected by KeyPoint would be shared with OPM—through the Secure Portal or otherwise. Plaintiffs accordingly allege that the shared nature of KeyPoint's and OPM's operations made it foreseeable "that a breach of KeyPoint's systems would expose OPM's systems . . . to a successful cyberattack." Compl. ¶ 217.

KeyPoint further undermines its position by terming the Data Breaches "extraordinary" and "not foreseeable" in the same breath as arguing such incidents happen all the time, and are "frequently 'successful.'" KP Mot. at 37, 38 (citing Compl. ¶ 80). KeyPoint's argument proves too much. It is clear that the predictable result of inadequate data security practices is unauthorized access to data. This is especially true in the context of government security where KeyPoint and OPM were tasked with gathering and storing highly sensitive and valuable data. *E.g.*, Compl. ¶¶ 3, 79, 143, 147.

Federal courts have found data breaches reasonably foreseeable to defendants whose flawed security created conditions conducive to criminal acts. For example, one court stated:

> [Defendant] contends that the intervening acts of criminals broke the causal chain. . . . [¶] Because the security measures could have prevented the criminal acts committed by the skimmers, [defendant's] failure to implement such measures created a condition conducive to a foreseeable intervening criminal act. Accordingly, the skimmers' reasonably foreseeable intervening criminal act did not sever the causal chain.

In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011); *see also, e.g.*, *Target*, 64 F. Supp. 3d at 1309 (crediting allegations that "[a]lthough the third-party hackers' activities caused harm, Target played a key role in allowing the harm to occur.").

The wrongful death cases on which KeyPoint relies are inapposite. *See* KP Mot. at 36. The first concerned a relief worker who was murdered in Somalia after she had already been in East Africa on her own "for personal reasons"—the defendant aid organization that later hired her as a contractor "was in no better position to provide for [her] safety than" she was herself.

Workman v. United Methodist Comm. on Relief of Gen. Bd. of Glob. Ministries of United Methodist Church, 320 F.3d 259, 264 (D.C. Cir. 2003). Here, by contrast, when Plaintiffs turned over their personal information to Defendants, they had no choice but to rely on Defendants to keep their information safe and secure. Compl. ¶¶ 192, 221, 240, 273. Unlike in *Workman*, KeyPoint and OPM were the *only* parties in a position to guard against the harm that occurred.

Nor can KeyPoint take solace in *Romero v. National Rifle Association of America, Inc.*, 749 F.2d 77 (D.C. Cir. 1984). In *Romero*, an NRA employee kept his handgun and ammunition in a closet in his office at work. *Id*. at 78. Four burglars broke into the NRA offices and stole the gun and some ammunition. *Id*. Four days later one of the burglars used the gun to rob and murder a man. *Id*. The estate of the murdered man sued the NRA and its employee for negligence, but the chain of causation was too attenuated to support tort liability. *Id*. at 80–81. By contrast, the causal chain in this case is not an unlikely series of events: KeyPoint's negligent failure to secure its systems led directly to the theft and misuse of Plaintiffs' private information.

Accepting KeyPoint's no-duty argument would weaken the incentives for entities that store sensitive private information to invest in needed electronic security. As the court in *Home Depot* stated, "[t]o hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk." 2016 WL 2897520, at *4. The court's reasoning has added force where the information collected was not payment card information for retail purchases, but highly sensitive personal and medical information (including fingerprints) for possible government employment and security clearances. A credit card number can be modified and a compromised card replaced. In contrast, Social Security numbers and other

sensitive personal information are irreplaceable. But the ruling sought by KeyPoint—that the government and its contractors are under no obligation to safeguard even the most sensitive personal information—could discourage public service by creating the perception, if not the likelihood, that very private, embarrassing, and potentially damaging personal facts may be exposed to unknown criminals on the black market, instead of being held in confidence.

2. Plaintiffs Sufficiently Plead Breach and Injury.

KeyPoint next objects that cyberattacks are so common that Plaintiffs "cannot reasonably *assume* that the cyber-attacks at issue were the result of some breach of duty," and "Plaintiffs have simply failed to *establish* that Plaintiffs suffered any cognizable injuries that were caused by KeyPoint." KP Mot. at 38, 39 (emphases added). Plaintiffs' allegations are more than sufficient to make out their case for causation and damages. KeyPoint's objections, in contrast, assume contrary facts that *KeyPoint* would need to prove to escape liability.

On a motion to dismiss, Plaintiffs' factual allegations indicating that KeyPoint breached its duty of care, and that such breach was a cause of harm, must be taken as true. *Atherton*, 567 F.3d at 677. First, the complaint alleges KeyPoint's unreasonable failures to:

> (a) secure its systems for gathering and storing GII, despite knowing of their vulnerabilities; (b) comply with industry-standard data security practices; (c) perform requisite due diligence and supervision in expanding its workforce; (d) encrypt GII at collection, at rest, and in transit; (e) employ adequate network segmentation and layering; (f) ensure continuous system and event monitoring and recording; and (g) otherwise implement security policies and practices sufficient to protect Plaintiffs' and Class members' GII from unauthorized disclosure.

Compl. ¶ 223. Second, KeyPoint's unreasonable nine-month delay in causing notice of the KeyPoint Breach to be provided to its victims forms an additional basis for Plaintiffs' claim of breach of duty. *Id*. ¶¶ 220, 224, 226. Third, the complaint describes how the KeyPoint security

deficiencies caused the theft of KeyPoint user credentials and Plaintiffs' personnel files, resulting in harm to Plaintiffs. *Id*. ¶¶ 4, 76, 163, 217, 223, 225, 228; *see also supra* Section I.A.2.

Rather than being unadorned, Plaintiffs' allegations provide "sufficient factual matter" in addition to the claim elements to give KeyPoint notice of the facts underlying Plaintiffs' negligence claims. *Iqbal*, 556 U.S. at 678. KeyPoint's attempt to convert questions of fact into grounds for dismissal on the pleadings should be rejected.

3. The Economic Loss Rule Does Not Bar Plaintiffs' Negligence Claims.

In two short paragraphs, KeyPoint argues that the economic loss rule bars Plaintiffs' claims for negligence. *See* KP Mot. at 39–40. This rule seeks to ensure that tort law does not displace the enforcement of contracts: to this end, it "*generally* provides that a contracting party who suffers purely economic consequences must seek his remedy in contract and not in tort." *Home Depot*, 2016 WL 2897520, at *3 (emphasis added) (citation omitted). Despite KeyPoint's efforts to portray the economic loss rule as if it were absolute, it has "important limits" directly implicated here. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255, 302–03 (2005). The facts of this case—the nature of the services KeyPoint provided; the uniquely private information Plaintiffs disclosed—prevent application of the economic loss rule. Most notably, KeyPoint forgets that "[w]here a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty." *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co.*, 636 N.E.2d 503, 514 (Ill. 1994). And where KeyPoint denies the existence of a contract (*see* KP Mot. at 43–44) it should not be heard to argue that recovery is unavailable in tort law.

D.C. law does not govern Plaintiffs' common-law claims against KeyPoint. *See supra* Section VI.A. Assessment of the economic loss rule, therefore, properly proceeds under the laws

of each Plaintiff's home state. Plaintiffs here reside in 24 states. For the assistance of the Court, Plaintiffs submit an Appendix of Law showing the treatment of the economic loss rule in each of these states. In nine of them—Alabama, Arizona, Florida, Michigan, Mississippi, North Carolina, Oklahoma, Tennessee, and Wisconsin—the doctrine is either not recognized or recognized only in limited circumstances not present here, such as a products liability suit or a contract for the sale of goods. In the states that at least arguably recognize the economic loss rule under other circumstances, relevant exceptions preclude its application here.

Eleven states—Georgia, Illinois, Kansas, Nevada, New Hampshire, New Mexico, New York, Texas, Utah, Virginia, and Washington—recognize an exception based on "independent duty." In these states, when "an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule." *Home Depot*, 2016 WL 2897520, at *3 (citation omitted). As the Utah Supreme Court instructed: "Where the economic loss rule is at issue, the initial inquiry becomes whether a duty exists independent of any contractual obligations between the parties. If we find that an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule." *Davencourt at Pilgrims Landing Homeowners Ass'n v. Davencourt at Pilgrims Landing, LC*, 221 P.3d 234, 244 (Utah 2009) (quotation marks and citations omitted).[21]

[21] There is an additional wrinkle to this exception under Illinois law: the economic loss doctrine is inapplicable where the defendant breached an independent duty *and* the product of the parties' relationship was "something intangible," *e.g.*, as here, a job or security clearance. *Congregation of the Passion*, 636 N.E.2d at 514–15; *but see Michaels Stores*, 830 F. Supp. 2d at 529–30 (erroneously treating this exception as being limited to professional malpractice claims

[Footnote continued on next page….]

This exception applies because KeyPoint breached an independent duty to guard against a foreseeable risk of harm. *Home Depot* demonstrates that this conclusion is correct. The court there determined that an independent duty "barr[ed] application of the economic loss rule" under Georgia law because, "even though there is a contract between the card issuers and the Plaintiffs," Home Depot owed the plaintiffs a duty not to subject them to an unreasonable risk of harm by exposing their personal information to hackers. 2016 WL 2897520, at *3. Federal courts have routinely reached the same result. *See, e.g.*, *In re Syngenta AG MIR 162 Corn Litig.*, 131 F. Supp. 3d 1177, 1190 (D. Kan. 2015) ("[T]he Court recognizes [an independent] duty here, based on plaintiffs' allegations that [defendant] created an unreasonable risk of harm to plaintiffs by its conduct."); *see also Target*, 66 F. Supp. 3d at 1171–77 (applying exception in data breach setting to preserve various state-law claims).

Here, every relevant state with an "independent duty" exception recognizes an independent common-law duty to avoid creating an unreasonable risk of harm.[22] This is precisely the duty that Plaintiffs allege KeyPoint breached. Compl. ¶¶ 217–21. Moreover, "[a] legal duty sufficient to support liability in negligence can be predicated on a duty imposed by a valid statutory enactment[.]" *Bouboulis v. Scottsdale Ins. Co.*, 860 F. Supp. 2d 1364, 1380 (N.D.

---

notwithstanding the Illinois Supreme Court's use of the phrase "service industry" and other expansive language to define the exception in *Congregation of the Passion*).

[22] *See, e.g.*, *Widlowski v. Durkee Foods, Div. of SCM Corp.*, 562 N.E.2d 967, 968 (Ill. 1990) ("[E]very person owes a duty of ordinary care to all others to guard against injuries which naturally flow as a reasonably probable and foreseeable consequence of an act, and such a duty does not depend upon contract . . . or the proximity of relationship, but extends to remote and unknown persons."); *accord FGA, Inc. v. Giglio*, 278 P.3d 490, 501 (Nev. 2012); *Walls v. Oxford Mgmt. Co.*, 633 A.2d 103, 104 (N.H. 1993); *Davis v. Board of Cnty. Comm'rs of Doña Ana Cnty.*, 987 P.2d 1172, 1178 (N.M. Ct. App. 1999); *Midwest Emp'rs Cas. Co. ex rel. English v. Harpole*, 293 S.W.3d 770, 776 (Tex. App. 2009); *Malan v. Lewis*, 693 P.2d 661, 672 n.15 (Utah 1984); *Rice v. Turner*, 62 S.E.2d 24, 26 (Va. Ct. App. 1950); *Parrilla v. King Cnty.*, 157 P.3d 879, 884 (Wash. Ct. App. 2007); *Alvarado v. Sersch*, 662 N.W.2d 350, 353 (Wis. 2003).

Ga. 2012) (citation omitted). KeyPoint had an independent statutory duty to maintain reasonable data security under FCRA and state statutes. *See supra* pp. 64–65 & fn. 20; *infra* Section VII.A.

In addition, other exceptions independently bar application of the economic loss doctrine.[23] With respect to the claims in the remaining four states—California, Idaho, Indiana, and Pennsylvania—the "special relationship" or "unique circumstances" exceptions apply because this case involves confidentiality and the repose of a special trust. *See, e.g.*, *Target*, 66 F. Supp. 3d at 1175–76 ("Pennsylvania recognizes a 'special relationship' exception in situations involving 'confidentiality [or] the repose of special trust' . . . . Plaintiffs' allegations here are that they reposed trust in Target or that Target bore a fiduciary-like responsibility to safeguard their financial information. Plaintiffs have plausibly pled the existence of a special relationship") (citation omitted).[24] Like the plaintiffs in *Target*, Plaintiffs here allege a special relationship with the company that maintained their private information—KeyPoint. Compl. ¶ 221.[25]

Thus, under the law of each of the Plaintiffs' home states, the economic loss doctrine is not an impediment to Plaintiffs' negligence claims.

---

[23] For example, in Illinois and elsewhere, the economic loss doctrine does not apply to negligent misrepresentation claims. *Moorman Mfg. Co. v. National Tank Co.*, 435 N.E.2d 443, 451–52 (Ill. 1982); *see generally* Plaintiffs' Appendix of Law Regarding the Economic Loss Rule.

[24] *See also J'Aire Corp. v. Gregory*, 598 P.2d 60, 62–63 (Cal. 1979) (recognizing special relationship exception); *Indianapolis-Marion Cnty. Pub. Library v. Charlier Clark & Linard, P.C.*, 929 N.E.2d 722, 736 (Ind. 2010) (directing Indiana courts to "be open" to applying appropriate exceptions, including, "for purposes of illustration only," where a defendant has breached a fiduciary duty or negligently misstated material facts). In Idaho, unique circumstances requiring a reallocation of risk also prevent application of the economic loss doctrine. *Just's, Inc. v. Arrington Const. Co.*, 583 P.2d 997, 1005 (Idaho 1978).

[25] Even if D.C. law were to apply, it too recognizes the special relationship exception. *See Aguilar v. RP MRP Wash. Harbour, LLC*, 98 A.3d 979, 984–85 & n.3 (D.C. 2014). In *Target*, the court applied *Aguilar*—KeyPoint's only case in support of its economic loss argument—to hold that dismissing negligence claims under D.C. law without further factual development relating to the data breach would be improper. 66 F. Supp. 3d at 1172–73.

C. The Complaint States a Claim for Negligent Misrepresentation and Concealment.

KeyPoint argues, without citation to relevant authority, for dismissal of the claim for negligent misrepresentation and concealment. *See* KP Mot. at 40–41. KeyPoint contends that Plaintiffs' allegations of reliance on OPM's representations in Standard Forms 85, 85P and 86 are insufficient. *Id.* at 41.

The elements of negligent misrepresentation are "(1) the defendant's negligent supply of false information to foreseeable persons, known or unknown; (2) such persons' reasonable reliance upon that false information; and (3) economic injury proximately resulting from such reliance." *Marquis Towers, Inc. v. Highland Grp.*, 593 S.E.2d 903, 906 (Ga. Ct. App. 2004) (citation omitted). The reasonable reliance element generally involves fact questions for the jury. *Stanford v. Owens*, 265 S.E.2d 617, 622 (N.C. Ct. App. 1980); *Chapman v. Skype Inc.*, 162 Cal. Rptr. 3d 864, 876 (Cal. Ct. App. 2013). "In determining whether justifiable reliance exists in a particular case, a fact finder should consider whether the person making the representation held or appeared to hold unique or special expertise; whether a special relationship of trust or confidence existed between the parties; and whether the speaker was aware of the use to which the information would be put and supplied it for that purpose." *Kimmell v. Schaefer*, 675 N.E.2d 450, 454 (N.Y. 1996); *cf.* Compl. ¶ 221 (allegations of special relationship).

KeyPoint's Privacy Policy misrepresented the level and quality of protection Plaintiffs' information received:

> KeyPoint disseminates its Privacy Policy on the Internet. The policy states that . . . KeyPoint is required by the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA"), to maintain the confidentiality of all consumer information. KeyPoint's Privacy Policy states that KeyPoint safeguards confidential consumer information from unauthorized internal and external disclosure, by maintaining a secure network, limiting access to KeyPoint's computer terminals and files, and maintaining backup data

> in encrypted form.

Compl. ¶ 77; *compare id.* ¶ 223 (detailing serious problems with KeyPoint's data security).

Plaintiffs allege that they relied on KeyPoint's false assurances of data protection and related omissions when they agreed to turn over their private information:

> KeyPoint's suppression and misrepresentation of material facts induced Plaintiffs and KeyPoint Subclass members to provide KeyPoint with their sensitive personal information or to permit KeyPoint to access their sensitive personal information. Had KeyPoint disclosed the inadequacy of its security measures, Plaintiffs and KeyPoint Subclass members would not have provided KeyPoint with their sensitive personal information or permitted KeyPoint to access their sensitive personal information.

Compl. ¶ 237.

KeyPoint's argument disregards these allegations, not to mention Plaintiffs' claim that KeyPoint is liable for *concealing* that its data security was not capable of protecting their information and the credentials used to gain access to it on KeyPoint's and OPM's systems. Compl. ¶¶ 230–38. Reliance is *presumed* where, as here, a plaintiff alleges the suppression of material facts—that is, facts that a reasonable person in the plaintiff's position would regard as important to the decision or transaction in question. *See* Restatement (Second) of Torts § 537. In the words of the Supreme Court, in a case "involving primarily a failure to disclose, positive proof of reliance is not a prerequisite to recovery. All that is necessary is that the facts withheld be material . . . ." *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128, 153 (1972). Further, "materiality is generally a question of fact unless the fact misrepresented is so obviously unimportant that the jury could not reasonably find that a reasonable man would have been influenced by it." *In re Tobacco II Cases*, 207 P.3d 20, 39 (Cal. 2009) (quotation marks and citations omitted); *see* Compl. ¶¶ 234, 237 (allegations relating to materiality).

The last paragraph of KeyPoint's negligent misrepresentation argument twists Plaintiffs'

complaint to imply that KeyPoint cannot be charged with constructive knowledge of its security failings at the time it released its misleading Privacy Policy. *See* KP Mot. at 41. Plaintiffs disagree, and for present purposes, the Court must draw reasonable inferences in favor of the pleading party. Moreover, Plaintiffs relied on KeyPoint's material misrepresentations and omissions when they provided their information, not "when the attack was detected" by KeyPoint. *Id.*; *compare* Compl. ¶ 237. The nine months that went by before KeyPoint discovered the breach of its systems are evidence of negligence, not its absence.

Plaintiffs' claim based on KeyPoint's negligent misrepresentations and concealment is the type of claim that has previously been recognized in data breach cases. *See, e.g.*, *In re Zappos.com, Inc.*, No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3–4 (D. Nev. Sept. 9, 2013). The claim here is well-pled.

D. The Complaint States a Claim for Invasion of Privacy.

Plaintiffs allege KeyPoint's misconduct caused the exposure, extraction, and loss of their highly sensitive private information, including the identities of past sexual partners; lie-detector test results; psychological and emotional health information; responses to inquiries concerning marital troubles, gambling compulsions, and past illicit drug and alcohol use; arrest records; private facts about children, other immediate family members, and relatives; and information relating to criminal and non-criminal legal proceedings. Compl. ¶¶ 144–47. It was quite reasonable for Plaintiffs to be highly offended by KeyPoint's unauthorized disclosure of their private, intimate information to unknown third parties. The complaint also alleges that KeyPoint's reckless acts and omissions caused this intrusion. *Id.* ¶¶ 242, 244. Consequently, KeyPoint's invasion of Plaintiffs' privacy is actionable at common law.

KeyPoint characterizes Plaintiffs' stolen information as not being of the kind worthy of

concern or protection under the invasion of privacy tort. *See* KP Mot. at 41. KeyPoint thus exhibits the same blasé attitude toward Plaintiffs' privacy rights that led to the exposure of their information in the first place. Its arguments fare no better on the merits.

To begin with, while the invasion of privacy tort normally involves one of the four distinct torts outlined by KeyPoint (*see* KP Mot. at 41), the tort admits of a wide and evolving variety of avenues by which a plaintiff's privacy may be invaded. *See* Restatement (Second) of Torts §§ 652A, 652B. The Restatement recognizes that with the rise of "various types of governmental interference and the compilation of elaborate written or computerized dossiers," application of the invasion of privacy cause of action to protect against such modes of privacy infringement may be increasingly warranted. Restatement (Second) of Torts § 652A cmt. c. Indeed, that a non-traditional means is used to invade an individual's privacy suggests, if anything, that the invasion is actionable: "If the means used is abnormal in character for gaining access to private information, then the intrusion is likely to be actionable regardless of the purpose." Prosser & Keeton on the Law of Torts § 117 at 856 (5th ed.). Courts in this District have long recognized that with the progression of "[m]odern life" and technology, the common law can and should afford protection of "the individual who desires . . . freedom from intrusion into his private life." *Peay v. Curtis Publ'g Co.*, 78 F. Supp. 305, 309 (D.D.C. 1948).

In this case, Plaintiffs' claim fits squarely within one of the four tort causes of action that have traditionally protected the privacy of individuals: Plaintiffs allege that KeyPoint intruded upon their seclusion and repose in the privacy of their highly personal information. KeyPoint's argument that a physical intrusion is an element of this tort is without merit. *See* KP Mot. at 42. The case upon which KeyPoint principally relies, *Wolf v. Regardie*, makes clear that a defendant need only have intruded "physically *or otherwise*" upon the "solitude or seclusion of another or

his private affairs or concerns[.]" 553 A.2d 1213, 1217 (D.C. 1989) (emphasis added) (citing Restatement (Second) of Torts § 652B). The tort is thus not confined to physical intrusions; liability may also be premised on "some other form of investigation or examination into [an individual's] private concerns, as by opening his private and personal mail, searching his safe or his wallet [or] examining his private bank account[.]" *Id*. cmt. b. The non-exhaustive set of examples in *Wolf*, too, includes "examining a plaintiff's private bank account[.]" 553 A.2d at 1218. Along similar lines, the California Supreme Court stated in dicta that a defendant that "obtain[s] unwanted access to data about" a plaintiff may be liable for the invasion. *Shulman v. Group W Prods., Inc*., 955 P.2d 469, 490 (Cal. 1998).

In addition, "[t]he intrusion itself makes the defendant subject to liability even though there is no publication or other use of any kind"—liability "does not depend upon any publicity given to the person whose interest is invaded or to his affairs." Restatement (Second) of Torts § 652B cmts. a, b. There is accordingly no merit to KeyPoint's unfounded contention that public dissemination is required to demonstrate liability. *See* KP Mot. at 42–43.

Likewise, the exposure of Plaintiffs' information alone injured them, regardless of whether that information has been or will ever be misused. *See, e.g.*, *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1984) (secret installation of hidden viewing devices in a skating rink bathroom was an invasion of privacy, without regard to whether they were used); *Hamberger v. Eastman*, 206 A.2d 239, 242 (N.H. 1964) (secret installation of a listening device in another's home was an invasion of privacy, without regard to whether it was used). In the data breach case of *Rowe v. UniCare Life & Health Insurance Co.*, the court upheld an invasion of privacy claim where an insurer had allowed the plaintiff's protected health information to be available online, temporarily, to the public, even though the plaintiff was unable to allege that

anyone had actually accessed his information. No. 09 C 2286, 2010 WL 86391, at *1, *9 (N.D. Ill. Jan. 5, 2010). The court explained that "in the case of an invasion of privacy action, 'proof of actual harm need not be of pecuniary loss' and actual harm may include damages for emotional distress." *Id*. at *9 (citing Restatement (Second) of Torts § 652H cmts. b & c). Here, Plaintiffs allege that KeyPoint's reckless security failures (Compl. ¶¶ 121, 222–23, 241–42) resulted in the theft of Plaintiffs' information (*id*. ¶¶ 7, 13–50, 117) and caused actual harm, such as emotional distress (*e.g.*, *id*. ¶ 244; *supra* Section I.A.1.e).

Nor can KeyPoint shield itself behind the acts of "criminal hackers" (KP Mot. at 42), because a defendant may be held liable for enabling an invasion of privacy completed by a third party. In *Carter v. Innisfree Hotel, Inc.*, a couple spent several hours having sex and lounging around naked in a hotel room, only to discover peep holes in the bathroom mirror. 661 So.2d 1174, 1177 (Ala. 1995). The Alabama Supreme Court held that the hotel's management company could be liable for intruding on the couple's privacy even if it was someone unaffiliated with the hotel who looked in on them, because the hotel had a duty to protect guests' privacy in their rooms. *Id.* at 1178–79. Plaintiffs in this case allege that KeyPoint had a duty to secure their private information and prevent unauthorized persons from accessing and removing it. *E.g.*, Compl. ¶¶ 77, 218. KeyPoint's failure to do so exposes it to liability for the consequent invasion of Plaintiffs' privacy. *Id*. ¶¶ 240–44.

KeyPoint's assertion that Plaintiffs gave up their information "voluntarily" (KP Mot. at 42) is a red herring. For one thing, Plaintiffs allege that KeyPoint's misrepresentations about reliable computer security induced them to submit their private information in the first instance. *E.g.*, Compl. ¶¶ 68–70, 77, 237. For another, whether their private information was or was not submitted voluntarily does not change Plaintiffs' objectively reasonable expectation—fostered in

part by KeyPoint's material misrepresentations and omissions—that this information would be kept safe and secure. *E.g., id.* ¶¶ 237, 255, 271, 273.

KeyPoint is reduced in the end to speculating that the information Plaintiffs proffered, which includes sexual histories and information about marital difficulties, extra-marital affairs, and drug use, could be accessed by other means. *See* KP Mot. at 43. Plaintiffs have, as an initial matter, alleged that this information was private; KeyPoint's idle speculation, therefore, remains just that. Moreover, if KeyPoint were correct that reasonable people did not expect the most intimate details of their lives to be kept secure, then there would have been no need for the representations of data security in KeyPoint's Privacy Policy. Compl. ¶ 77. KeyPoint does not, and cannot, explain why it provided those assurances if Plaintiffs' private information was nothing special. KP Mot. at 43. In any event, these are fact questions inappropriate for resolution here. *See Harms v. Miami Daily News, Inc.*, 127 So.2d 715, 718 (Fla. Dist. Ct. App. 1961); *Strickler v. National Broad. Co.*, 167 F. Supp. 68, 71 (S.D. Cal. 1958).

Finally, the allegations of the complaint state claims for invasion of privacy under both the common law and Article I, Section 1 of the California Constitution, which applies to the claims of plaintiffs from that state. Compl. ¶¶ 34, 43. *See Sheehan v. San Francisco 49ers, Ltd.*, 201 P.3d 472, 477–78 (Cal. 2009) (reciting elements of state constitutional cause of action and noting that it may be brought to protect "interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy')."); *Am. Acad. of Pediatrics v. Lungren*, 940 P.2d 797, 808 (Cal. 1997) (stating that "not only is the state constitutional right of privacy embodied in explicit constitutional language not present in the federal Constitution, but past California cases establish that, in many contexts, the scope and application of the state constitutional right of privacy is broader and more protective of privacy than the federal

constitutional right of privacy"). KeyPoint's authority applying this constitutional provision involved significantly lesser intrusions than here. *See* KP Mot. at 43 n.35. For instance, the plaintiff in *Ruiz v. Gap, Inc.* alleged only "an increased *risk* of privacy invasion, rather than an actual privacy invasion." 380 F. App'x 689, 693 (9th Cir. 2010) (emphasis added). While the court in *Low v. LinkedIn Corp.* found that it was "not clear" that any third party had successfully "de-anonymize[d]" the information, or "what information, precisely, these third parties ha[d] obtained," 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012), that is not the case here.

VII. THE STATUTORY CAUSES OF ACTION AGAINST KEYPOINT ARE WELL-PLED.

A. The Complaint States a Claim Under the Fair Credit Reporting Act.

Plaintiffs allege sufficient facts to establish KeyPoint's violations of sections 1681b and 1681e(a) of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA"). KeyPoint's derelict data security measures not only were a cause of the KeyPoint Breach but also permitted hackers to obtain the KeyPoint user credentials that were then used to hack into OPM's servers. Compl. ¶¶ 4–6, 249–51. It was by failing to secure these credentials that KeyPoint unlawfully made accessible to hackers the records stolen in the OPM Breaches. *Id*. ¶¶ 127–33.

KeyPoint's motion and appendix of law quote only section 1681(a) of FCRA to suggest, misleadingly, that the sole purpose of the statute is to "ameliorate harms caused by '[i]naccurate credit reports' and 'unfair credit reporting methods.'" KP Mot. at 23, App. A, Table 1. But a central purpose of FCRA is also "to require that consumer reporting agencies adopt reasonable procedures" to ensure "the confidentiality, accuracy, relevancy, and proper utilization of [consumers'] information." 15 U.S.C. § 1681(b). These statutory objectives have become more important with the advent of the Internet and other technological advances since FCRA's enactment in 1970. KeyPoint, however, conspicuously fails to acknowledge that FCRA

"require[s] . . . reasonable procedures" to ensure the "confidentiality" and "proper utilization" of consumers' credit-related information. 15 U.S.C. § 1681(b).

Under FCRA, "[e]very consumer reporting agency shall maintain reasonable procedures designed to avoid violations" of the Act, including section 1681b. 15 U.S.C. § 1681e(a). "The reasonableness of the procedures and whether the agency followed them will be jury questions in the overwhelming majority of cases." *Guimond v. Trans Union Credit Info. Co.*, 45 F.3d 1329, 1333 (9th Cir. 1995); *accord Cortez v. Trans Union, LLC*, 617 F.3d 688, 709 (3d Cir. 2010). FCRA creates a private right of action for willful or negligent noncompliance with these requirements. *Id*. §§ 1681n, 1681o; *see Boggio v. USAA Fed. Sav. Bank*, 696 F.3d 611, 615 (6th Cir. 2012); *Nelson v. Chase Manhattan Mortg. Corp.*, 282 F.3d 1057, 1059 (9th Cir. 2002).

KeyPoint does not deny that it is a consumer reporting agency (Compl. ¶¶ 77, 246); that the records at issue qualify as consumer reports (*id*. ¶ 246); or that the disclosure of Plaintiffs' information in the Data Breaches was for no purpose permitted under FCRA (*id*. ¶¶ 249–50). KeyPoint bases its challenge to the FCRA claim on a single assertion: "it is obvious . . . no reports were being 'furnished'" in the Data Breaches. KP Mot. at 23–24. But Plaintiffs' interpretation of "furnish" is not only plausible, it is correct.

As the executive agency charged with primary enforcement of FCRA, *see* 15 U.S.C. § 1681s(a), the Federal Trade Commission's interpretations of FCRA merit "considerable weight" and judicial deference. *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 844 (1984); *see also United States v. Mead Corp.*, 533 U.S. 218, 227–28 (2001). The FTC has pursued enforcement actions for violations of FCRA sections 1681b and 1681e where inadequate security led to data breaches that compromised consumer records. *See In the Matter of ACRAnet, Inc.*, No. C-4331, 2011 WL 479886 (FTC Feb. 3, 2011), ¶ 9 (alleging the defendant

violated FCRA when "[i]n multiple breaches, hackers accessed at least 694 consumer reports"); *In the Matter of SettlementOne Credit Corp.*, No. C-4330, 2011 WL 479885 (FTC Feb. 3, 2011), ¶ 10 (alleging the defendant violated FCRA when "[i]n multiple breaches, hackers accessed at least 784 consumer reports"); *In the Matter of Fajilan & Assocs., Inc.*, No. C-4332, 2011 WL 479887 (FTC Feb. 3, 2011), ¶ 10 (alleging the defendant violated FCRA when "[i]n multiple breaches, hackers accessed at least 323 consumer reports").

Commissioner Brill, writing separately, criticized these companies for their failure to protect consumers' information in terms that could apply equally to KeyPoint:

> The allegations indicate that respondents in these three matters treated their legal obligations to protect consumer information as a paper exercise. According to the complaint, respondents provided only a cursory review of security measures. Thereafter, respondents took no further action to ensure that their customers' security measures adequately protected the information in the consumer reports.

Statement of Commissioner Brill, in Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, No. C-4330, 2011 WL 3726287, at *10 (FTC Aug. 15, 2011). Commissioner Brill made clear, moreover, that FCRA applies to—and prohibits—inadequate data security measures:

> We . . . emphasize that in the future we will call for imposition of civil penalties against resellers of consumer reports who do not take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the Fair Credit Reporting Act ("FCRA"). . . . [¶] The FCRA requires respondents to take reasonable measures to ensure that consumer reports ***are given*** only to entities using the reports for purposes authorized by the statute. [Footnote] There is no doubt that such unauthorized access can result in grave consumer harm . . . .

Id. (emphasis added).

KeyPoint's argument to the contrary relies on an incomplete and selective sample of data breach cases brought under FCRA. *See* KP Mot. at 24 (citing *Willingham v. Global Payments, Inc.*, No. 12-cv-1157-RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013), and *Dolmage v.*

Combined Ins. Co. of Am., No. 14-cv-3809, 2015 WL 292947 (N.D. Ill. Jan. 21, 2015)). Neither court analyzed, much less revealed any awareness of, the determination of the FTC that the disclosure of consumer reports in data breach incidents *does* constitute an unlawful furnishment. *Cf. Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 70 (2007) (recognizing "the benefit of guidance from the courts of appeals or the Federal Trade Commission" in interpreting FCRA provisions). In *Harrington v. ChoicePoint Inc.*, by contrast, the court upheld claims under FCRA sections 1681b and 1681e(a) against a company alleged to have unlawfully communicated the private information of tens of thousands of individuals to third parties who posed as legitimate subscribers to "gain access" to the company's "internet-based data products." No. CV 05-1294 MRP (JWJx), 2005 WL 7979032, at *1–5 (C.D. Cal. Sept. 15, 2005). The court explained that sections 1681b and 1681e(a) "govern the manner and purpose under which a 'consumer reporting agency' ('CRA') may *make available* a 'consumer report' for use by third parties." *Id*. at *2 (emphasis added).[26]

KeyPoint insists that it did not commit a "deliberate" or "active" act of data transmission and therefore cannot be liable. KP Mot. at 24 (citations omitted). But, even if a deliberate or active act of data transmission were required, KeyPoint's argument rests on a factual inference that cannot be drawn in its favor at this point. Although "[p]recisely how the KeyPoint Breach occurred has not been disclosed" (Compl. ¶ 121), the complaint alleges that "an unknown person or persons obtained the user log-in credentials of a KeyPoint employee" which, thereafter, were

[26] The *Harrington* court focused its analysis on whether the compromised information qualified as consumer reports, as the parties do not appear to have raised the "furnishment" issue pressed by KeyPoint. *Id.* Courts have also approved the voluntary resolution of FCRA claims arising from data breaches. *See, e.g.*, *In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, No. 3:08-MD-01998, 2009 WL 5184352, at *10 (W.D. Ky. Dec. 22, 2009); *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 851 F. Supp. 2d 1040 (S.D. Tex. 2012).

used to perpetrate the OPM Breaches (*id*. ¶ 4). Whether the loss of the KeyPoint employee's credentials involved deliberate conduct is not presently known.

KeyPoint's statement that "[i]t would be absurd to claim that when a thief breaks into your car, you have 'furnished' him with a new car stereo" (KP Mot. at 24), is inapposite. Plaintiffs do not seek to hold KeyPoint liable for stealing their information, but, rather, for its unreasonable and unlawful failure to protect their information from disclosure to third parties. The flaw in KeyPoint's hypothetical is that the defendant's status as an intermediary can make a difference. Thus, for example, a bank employee who violates his job duties by recklessly divulging the access codes to teller drawers full of cash can rightly be understood to have furnished the cash to a person who subsequently uses those codes.

In sum, it is not KeyPoint's but the FTC's construction of "furnish" that comports with the word's standard meaning: "furnishing" does not require an "active" or "deliberate" transmission, or indeed any volitional act at all. *See* American Heritage Dictionary at 534 (1981) (to "furnish" is to "supply; give"); *cf. Taniguchi v. Kan Pac. Saipan, Ltd.*, 132 S. Ct. 1997, 2002 (2012) ("When a term goes undefined in a statute, we give the term its ordinary meaning.").[27] KeyPoint's two district court cases simply take it on faith that "furnishment" under FCRA requires a deliberate or volitional transmission. No such requirement, however, appears in the text of the statute. A plain English reading recognizes that furnishment occurs when consumer reports are supplied to third parties through inordinately lax data security. This is what the

[27] The Oxford English Dictionary quotes Winston Churchill's use of "furnish" to describe "a system which . . . had for long furnished mankind with its brightest dreams." New Shorter Oxford English Dictionary at 1045 (1993). Churchill's statement aptly demonstrates that the word "furnish" does not necessarily connote active or deliberate transmission by a "furnisher." (Churchill was referring to the medieval outlook, with its universality and spiritual focus.)

Federal Trade Commission concluded. This is the interpretation that furthers a core purpose of the statute—"to require that consumer reporting agencies adopt reasonable procedures" to ensure "the confidentiality . . . and proper utilization of [consumers'] information." 15 U.S.C. § 1681(b). As such, the FCRA claim should be upheld.

B. The Complaint States a Claim Under State Statutes Prohibiting Unfair or Deceptive Acts or Practices.

1. The UDAP Statutes Apply to KeyPoint's Alleged Conduct.

KeyPoint narrowly construes "trade and commerce" and "consumer transactions" in an attempt to defeat Plaintiffs' claims under twelve state statutes prohibiting unfair or deceptive acts or practices ("UDAP statutes"). *See* KP Mot. at 25; *cf.* Compl. ¶ 256. Yet courts applying these state laws have adopted a more liberal reading of these terms. *See, e.g.*, *Corona v. Sony Pictures Entm't*, No. 14-cv-9600, 2015 WL 3916744, at *8 (C.D. Cal. June 15, 2015) (denying motion to dismiss employee plaintiffs' data breach claims under Cal. Bus. & Prof. Code § 17200, *et seq.* (the "UCL")).[28] KeyPoint's claim that "it was not engaged in commerce" (KP Mot. at 25) is

[28] *See also GoHealth, LLC v. Simpson*, No. 13-cv-2334, 2013 WL 6183024, at *13–14 (N.D. Ill. Nov. 26, 2013) (815 Ill. Comp. Stat. Ann. 505/2, *et seq.*, applies to claims by non-consumers); *Windisch v. Hometown Health Plan, Inc.*, No. 08-cv-664, 2010 WL 786518, at *5–7 (D. Nev. Mar. 5, 2010) ("[C]onsumer fraud is not limited to traditional consumers" under Nev. Rev. Stat. Ann. § 598.0915, *et seq.*); *LaChance v. U.S. Smokeless Tobacco Co.*, 931 A.2d 571, 576–77 (N.H. 2007) ("Any person injured," within N.H. Rev. Stat. Ann. § 358-A:2, *et seq.*, calls for a broad application); *Navajo Nation v. Urban Outfitters, Inc.*, 935 F. Supp. 2d 1147, 1172–73 (D.N.M. 2013) (under N.M. Stat. Ann. § 57-12-2, *et seq.*, "any person" injured may sue, including non-consumers); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 951 F. Supp. 1224, 1231–32 (M.D.N.C. 1996) (endorsing application of N.C. Gen. Stat. Ann. § 75-1.1(a), *et seq.*, to non-consumer scenarios); *In re Rodriguez*, 218 B.R. 764, 784–86 (Bankr. E.D. Pa. 1998) (in context of a "self-help eviction" by a mortgagee, holding debtor entitled to damages under 73 Pa. Stat. § 201-2, *et seq.*, and citing legislative intent that the statute "must be liberally interpreted for the purpose of abating unfair and deceptive practices"); *In re Moon*, Nos. 96-4086, 96-42453, 1997 WL 34625685, at *21 (Bankr. E.D. Va. Dec. 17, 1997) (applying Va. Code Ann. § 59.1-200, *et seq.*, to debtor's claims arising from the construction of a home and finding the statute should be "construed broadly" to promote fair and ethical business practices); *Holiday Resort*

[Footnote continued on next page….]

mistaken. KeyPoint's background and security check services are its operative "trade" and it performs these services in furtherance of its commercial business. Compl. ¶ 254. The UDAP statutes define "commerce" broadly, in a way that clearly encompasses KeyPoint's business. *See, e.g.*, N.C. Gen. Stat. Ann. § 75-1.1(b) (defining "commerce" to "include[] all business activities, however denominated"); N.H. Rev. Stat. Ann. § 358-A:1 (defining trade and commerce to include "distribution of any services").

The complaint alleges that in the course of conducting its background check business KeyPoint failed to safeguard Plaintiffs' extremely personal information, contrary to the assurances it provided in its Privacy Policy. Compl. ¶ 255. Separate and apart from KeyPoint's deception, its disregard for the security of Plaintiffs' private information is actionable as unfair and unconscionable business conduct. *Klem v. Washington Mut. Bank*, 295 P.3d 1179, 1187 (Wash. 2013) (recognizing that "an act or practice can be unfair without being deceptive."); *see, e.g.*, Fla. Stat. Ann. § 501.204(1) (prohibiting "[u]nfair methods of competition, unconscionable acts or practices, and unfair *or* deceptive acts or practices") (emphasis added); 815 Ill. Comp. Stat. Ann. 505/2 ("Unfair methods of competition and unfair or deceptive acts or practices . . . in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby."); N.M. Stat. Ann. § 57-12-3 (prohibiting "unconscionable trade practices"). Courts applying these statutes have defined "unfair" business practices, in part, as those that offend established public policy; that are immoral, unethical, oppressive, unscrupulous or substantially injurious; or whose benefits are outweighed by their

---

Cmty. Ass'n v. Echo Lake Assocs., LLC, 135 P.3d 499, 505 (Wash. Ct. App. 2006) (finding tenants had standing to sue property owners under Wash. Rev. Code § 19.86.020, *et seq.*, as the statute has been held applicable to claims involving "no consumer relationship").

harmful effects. *See, e.g.*, *McKell v. Washington Mut., Inc.*, 49 Cal. Rptr. 3d 227, 240 (Cal. Ct. App. 2006); *CareerFairs.com v. United Bus. Media LLC*, 838 F. Supp. 2d 1316, 1324 (S.D. Fla. 2011); *Mellon v. Regional Tr. Serv. Corp.*, 334 P.3d 1120, 1126 (Wash. Ct. App. 2014). KeyPoint's failure to safeguard Plaintiffs' information violates public policy and satisfies these standards.

2. Plaintiffs' UDAP Claims Are Not Subject to Rule 9(b) But, in Any Event, Satisfy Its Pleading Standard.

Plaintiffs need not satisfy the heightened pleading standard of Rule 9(b) because neither fraud nor mistake is an element of Plaintiffs' UDAP claims. *See* KP Mot. at 26–27. "Because neither fraud nor mistake is an element of unfair conduct under Illinois' Consumer Fraud Act, a cause of action for unfair practices under the Consumer Fraud Act need only meet the notice pleading standard of Rule 8(a), not the particularity requirement in Rule 9(b)." *Windy City Metal Fabricators & Supply, Inc. v. CIT Tech. Fin. Servs., Inc.*, 536 F.3d 663, 670 (7th Cir. 2008); *see also Guerrero v. Target Corp.*, 889 F. Supp. 2d 1348, 1355 (S.D. Fla. 2012) (explaining that Florida's UDAP statute "was enacted to provide remedies for conduct outside the reach of traditional common law torts like fraud"—so "heightened pleading requirements of Rule 9(b)" do not apply). Here, KeyPoint may be found liable on a showing that its conduct was unfair.

To the extent Plaintiffs' UDAP claims also involve deception and material concealment, a "fraud by concealment claim can succeed without the same level of specificity required by a normal fraud claim" because "[i]n most cases, 'a plaintiff . . . will not be able to specify the time, place, and specific content of an omission as precisely as would a plaintiff in a false representation claim.'" *Anthem*, 2016 WL 3029783, at *35 (citations omitted). The court in *Anthem* upheld a claim that the defendant violated the UCL through its material omissions, where the plaintiffs alleged that they "would not have enrolled in Defendants' insurance and

health benefit services if they had known about Defendants' substandard data security practices." *Id*. at *35–36 (citing complaint). Similarly here, Plaintiffs allege that they "would not have provided KeyPoint with their sensitive personal information or permitted KeyPoint to access their sensitive personal information" had they known that KeyPoint's data security practices were inadequate. Compl. ¶ 237.

The cases KeyPoint cites in arguing that a heightened pleading standard applies to the Illinois and California statutory claims are readily distinguishable. Allegations of intentional omissions were at issue in *Pirelli Armstrong Tire Corp. Retiree Med. Benefits Trust v. Walgreen Co.*, 631 F.3d 436, 447 (7th Cir. 2011), but the complaint in this case does not assert claims for intentional misrepresentations or omissions (common-law fraud) by KeyPoint. The same distinction renders *Kearns v. Ford Motor Co.* inapplicable. 567 F.3d 1120 (9th Cir. 2009). In *Kearns* the court reasoned that the complaint was based "entirely on a unified fraudulent course of conduct," such that fraud was an "essential element" of the plaintiff's UCL claim. *Id*. at 1124–27. Not so here. Plaintiffs' complaint does not sound in fraud. Plaintiffs allege unfair and deceptive practices on the part of KeyPoint. Compl. ¶ 255.

Finally, even if Rule 9(b) were to apply, Plaintiffs' allegations meet it.

- "KeyPoint's Privacy Policy states that KeyPoint safeguards confidential consumer information from unauthorized internal and external disclosure, by maintaining a secure network, limiting access to KeyPoint's computer terminals and files, and maintaining backup data in encrypted form." Compl. ¶ 77.

- These representations were misleading: KeyPoint's data security measures departed from commercial norms and contained several severe deficiencies. *Id.* ¶¶ 222–23.

- KeyPoint owed a duty to communicate material facts to Plaintiffs regarding the security of their information, but neglected to do so. *Id*. ¶¶ 231–37.

- Even after KeyPoint's information systems were breached in December 2013, KeyPoint represented for several months that its systems were secure, and continued to accept individuals' personal information for use in background and security clearance

checks. *Id*. ¶¶ 77, 114, 117, 226, 255, 263.

These allegations adequately set forth the particulars of KeyPoint's deception. *See, e.g.*, *Target*, 66 F. Supp. 3d at 1162–63 (finding a duty to disclose under the UDAP statutes of 18 states based on allegations that Target "knew that its customers' data was sensitive and should be protected, knew that its systems were inadequate to protect that data, and continued to accept [its customers' data] after it knew or should have known that the systems were susceptible to breach or had been breached.").

3. Plaintiffs Adequately Allege That KeyPoint's Violations of the UDAP Statutes Injured Them.

KeyPoint's remaining challenges fare no better. First, Plaintiffs have already discussed how, based upon the complaint's particularized allegations of fact, Plaintiffs' injuries are traceable to KeyPoint's violations—whether their information was exposed in the KeyPoint Breach or in the OPM Breaches perpetrated using credentials that KeyPoint failed to secure. *See supra* Section I.A.2.b. Second, KeyPoint's statutory causation argument attacks the straw man of reliance. *See* KP Mot. at 28. The law is clear, however, that Plaintiffs may obtain relief based solely on a showing that KeyPoint's security failures were unfair. *See McKell*, 49 Cal. Rptr. 3d at 238–39; *Klem*, 295 P.3d at 1187.

To the extent the UDAP claims rest on KeyPoint's material misrepresentations and omissions, reliance is not generally a required element of such claims and the complaint adequately sets forth the chain of causation. "Nationally, it is clear that most state consumer protection statutes have dispensed with the onerous burden of requiring that private plaintiffs prove individual reliance and many, if not most, of the remaining elements of fraud." Seth William Goren, *A Pothole on the Road to Recovery: Reliance and Private Class Actions Under Pennsylvania's Unfair Trade Practices and Consumer Protection Law*, 107 Dick. L. Rev. 1, 13

(2002) (citing cases); *see, e.g.*, *State v. Commerce Commercial Leasing, LLC*, 946 So. 2d 1253, 1258 (Fla. Dist. Ct. App. 2007); *Empire Home Servs., Inc. v. Carpet Am., Inc.*, 653 N.E.2d 852, 854 (Ill. App. Ct. 1995) ("[T]he Consumer Fraud Act does not require actual reliance.").

In many states, moreover, only a tendency or likelihood to deceive need be shown. *See, e.g.*, *Morgan v. AT & T Wireless Servs., Inc.*, 99 Cal. Rptr. 3d 768, 784–85 (Cal. Ct. App. 2009); *Cullen v. Valley Forge Life Ins. Co.*, 589 S.E.2d 423, 431 (N.C. Ct. App. 2003); *Page & Wirtz Constr. Co. v. Solomon*, 794 P.2d 349, 352–54 (N.M. 1990); *Commonwealth v. Bell Tel. Co. of Pa.*, 551 A.2d 602, 603–04 (Pa. Commw. Ct. 1988). Actual reliance is now required under California's UCL, but Plaintiffs satisfy that element by alleging that they would have refrained from providing their information had KeyPoint disclosed the truth about its data security. Compl. ¶ 237; *see Anthem*, 2016 WL 3029783, at *35–36.

KeyPoint's causation argument substitutes colorful words like "dooms" for reasoned argument grounded in the complaint. KP Mot. at 28–29. Plaintiffs nowhere allege that KeyPoint, "at the earliest, would have known about KeyPoint cyber-attack in September 2014." *Id*. at 29. That attack occurred the previous calendar year. Compl. ¶¶ 114, 224. That KeyPoint did not learn of it for nine months bolsters Plaintiffs' statements regarding KeyPoint's wrongdoing, including that KeyPoint "unreasonably delayed" providing Plaintiffs with notice of this intrusion. *Id*. ¶ 261. KeyPoint seems to suggest that its own failure to promptly discover the breach of its systems kept it from notifying the victims in time to do any good, thus rendering it immune for unfair and deceptive conduct. *See* KP Mot. at 29. But KeyPoint not only could and should have discovered the KeyPoint Breach earlier, it could and should have taken concrete steps to avoid this breach (which would have avoided Plaintiffs' injuries) and, at the very least, warned Plaintiffs that their personal information was at risk even earlier than that. Instead, after

its systems were infiltrated, KeyPoint did not correct its Privacy Policy misrepresentations and continued to gather information. Compl. ¶¶ 77, 255(e).

KeyPoint's convoluted argument takes nothing away from Plaintiffs' allegations that their injuries flow from KeyPoint's systemic failures before, during, and after the December 2013, May 2014, and October 2014 Data Breaches; were the foreseeable consequences of those failures; and would not have occurred but for those failures. Compl. ¶¶ 4, 114, 127, 222–28.

C. The Complaint States a Claim Under State Statutes Requiring Prompt Disclosure of Data Breach Incidents.

1. Plaintiffs' Claims Under the Data Breach Acts Are Not Preempted.

Nothing in federal law conflicts with Plaintiffs' claims under state laws requiring prompt notification of data breach incidents. It should come as no surprise, therefore, that KeyPoint can cite no authority to support its argument for federal preemption. KeyPoint's argument for preemption also raises questions of fact that could not be resolved on a motion to dismiss and would not, in any case, overcome the strong presumption against preemption of state laws enacted to protect citizens. *See Greenwich Ins. Co. v. Mississippi Windstorm Underwriting Ass'n*, 808 F.3d 652, 655 (5th Cir. 2015) (proponent of preemption bears the burden). Unlike a statute or duly promulgated regulation, the OMB Breach Notification Memorandum, which is an internal agency memorandum, and the two policy guidance documents cited by KeyPoint, lack the force of law. Furthermore, even assuming KeyPoint's cited materials could have preemptive effect—which they cannot—these materials fail to satisfy the conflict preemption standard. *See English v. General Elec. Co.*, 496 U.S. 72, 79 (1990) (holding that there is no conflict preemption except "where it is impossible for a private party to comply with both state and federal requirements, or where state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.'") (citations omitted).

a. KeyPoint's Preemption Argument Fails to Overcome the Strong Presumption Against Preemption.

The strong presumption against preemption of historic state police powers may be overcome only by "clear and manifest" congressional intent. *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996). "[C]onsumer protection law is a field traditionally regulated by the states[.]" *General Motors Corp. v. Abrams*, 897 F.2d 34, 41 (2d Cir. 1990); *see also Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947). In such a field, "preemption of state law by federal statute or regulation is not favored 'in the absence of persuasive reasons—either that the nature of the regulated subject matter permits no other conclusion, or that the Congress has unmistakably so ordained.'" *Chicago & N.W. Transp. Co. v. Kalo Brick & Tile Co.*, 450 U.S. 311, 317 (1981) (citation omitted).

KeyPoint points to no federal legislation that expressly preempts state data breach laws. FISMA, the federal statute invoked by KeyPoint (KP Mot. at 30), contains no language so much as implying a congressional intent to preempt state law. FISMA requires federal agencies to develop and implement "information security program[s]" that include "procedures for detecting, reporting, and responding to security incidents[.]" 44 U.S.C. § 3554(b)(7). Several of the state laws at issue were already on the books when Congress enacted this FISMA provision, in 2012, yet Congress expressed no intent—let alone clear and manifest intent—to preempt any of these state laws. *See* Ga. Code Ann. § 10-1-912(a) (effective May 24, 2007); Mich. Comp. Laws Ann. § 445.72(1) (effective Apr. 1, 2011); N.H. Rev. Stat. Ann. § 359-C:20(I)(a) (effective Jan. 1, 2007); N.C. Gen. Stat. Ann. § 75-65(a) (effective Oct. 1, 2009); Va. Code Ann. § 18.2-186.6(B) (effective July 1, 2008); Wis. Stat. Ann. § 134.98(2) (effective Mar. 28, 2008).

The absence of an express preemption clause evidences Congress's intent for the federal information security regime not to displace state laws, but to complement them. *See Wyeth v.*

Levine, 555 U.S. 555, 574–75 (2009). In fact, Congress made clear that it intended for FISMA to "provide for development and maintenance of *minimum* controls required to protect Federal information and information systems"—*i.e.*, a floor, not a ceiling. 44 U.S.C. § 3551(3) (emphasis added).

b. There Is No Conflict with Federal Law.

i. The Agency Materials Relied on by KeyPoint Lack Preemptive Force.

The internal agency documents that form the basis for KeyPoint's preemption argument do not manifest any intent to preempt state law and, moreover, lack the force of law. *See* KP Mot. at 30–31. While both federal statutes and regulations with the force of law can preempt contrary state law, *Fidelity Fed. Sav. & Loan Ass'n v. de la Cuesta*, 458 U.S. 141, 153 (1982), agency guidance cannot—only a binding norm issued after notice and comment can preempt contrary state law. This requirement respects the sovereignty of the States: "Limiting the preemptive power of federal agencies to exercises of formal rulemaking authority, then, ensures that the states will have enjoyed these protections before suffering the displacement of their laws." *Good v. Altria Grp., Inc.*, 501 F.3d 29, 51 (1st Cir. 2007), *aff'd*, 555 U.S. 70 (2008); *see, e.g.*, *Fellner v. Tri-Union Seafoods, L.L.C.*, 539 F.3d 237, 245 (3d Cir. 2008) ("We decline to afford preemptive effect to less formal measures lacking the 'fairness and deliberation' which would suggest that Congress intended the agency's action to be a binding and exclusive application of federal law. Courts with good reason are wary of affording preemptive force to actions" absent such circumstances) (citing, *inter alia*, *Wabash Valley Power Ass'n, Inc. v. Rural Electrification Admin.*, 903 F.2d 445, 453 (7th Cir. 1990)).

KeyPoint does not claim that the internal agency documents it cites are duly promulgated regulations. Nor has KeyPoint pointed to norms promulgated in compliance with the notice and

comment rulemaking provisions of the APA. *See* 5 U.S.C. § 553. Instead, it refers only to internal agency guidance documents. Such documents are generated by and subject only to internal deliberations of the executive branch. They have no preemptive effect.

Holk v. Snapple Beverage Corp., 575 F.3d 329 (3d Cir. 2009), on which KeyPoint relies, requires this result. *See* KP Mot. at 31 n.23. The court in *Holk* held that an agency policy regarding the use of the term "natural" on product labels, and agency letters applying that policy, were informal guidance that therefore lacked the "force of law required to preempt conflicting state law." 575 F.3d at 340–42. Similar preemption arguments divorced from a statute or formal rule have met with the same result. *See, e.g.*, *Wyeth*, 555 U.S. at 577 (holding that a preamble to a regulation lacks preemptive effect in the absence of formal rulemaking); *Fellner*, 539 F.3d at 241, 251–52 (neither a letter from the agency stating that the suit was preempted, nor agency enforcement guidelines and advisories, had any preemptive effect); *United States v. Ferrara*, 847 F. Supp. 964, 969 (D.D.C. 1993) (concluding that "a policy memorandum issued by the head of an executive agency simply is not the equivalent of 'federal law'" where the "memorandum was neither promulgated pursuant to notice and comment rulemaking nor published in the Federal Register").

The regulations at issue in *Geier v. American Honda Motor Co.*, 529 U.S. 861 (2000), by contrast, had preemptive effect because they were duly promulgated regulations with the force of federal law. *See* KP Mot. at 29, 32. In *Geier*, a federal statute mandated that the Secretary of Transportation issue motor vehicle safety standards that "shall be practicable, shall meet the need for motor vehicle safety, and shall be stated in objective terms." 529 U.S. at 889 (citing 15 U.S.C. § 1392(a) (recodified at 49 U.S.C. § 30111(a)). The Secretary after notice and comment rulemaking promulgated regulations implementing this statute. *Geier*, 529 U.S. at 889–90.

Called upon to address a conflict between one of these regulations, which expressly permitted the use of competing safety alternatives, and an attempt to impose common-law liability on automakers for choosing one of these alternatives in preference to the other, the Supreme Court held that the state-law claim "actually conflict[ed]" with the federal regulation. *Id*. at 874–76.

In this case, there is neither an intrusive regulatory environment nor any federal regulation or other binding source of federal law on point. No federal regulation conflicts with (or relates to) Plaintiffs' claims under the state data breach acts. The materials referenced by KeyPoint are similar to internal protocols and manuals, were not subject to formal rulemaking, and cannot divest the states of their historic police powers.

ii. The Agency Materials Relied on by KeyPoint Neither Refer to Nor Supersede the Data Breach Acts.

Even if these internal documents did have the force of law, preemption would be inappropriate because these documents do not conflict with state data breach laws. Like FISMA, OPM's internal policies set a floor, not a ceiling, for information security programs. Far from preempting state law, these policies do no more than "establish[] *minimum* standards for the protection of PII." OPM, *Policy on the Protection of Personally Identifiable Information (PII)* § 3.1.1 (2012) (emphasis added) ("OPM 2012 Policy"); OPM, *Policy on the Protection of Personally Identifiable Information (PII)* § 3.1.1 (2014) ("OPM 2014 Policy"). These minimum standards do not, either expressly or impliedly, preclude federal contractors from providing notice of data breaches. The policies state only that an OPM division "will ensure all required notifications to the affected Subject(s) are made within three days of determination[.]" OPM 2012 Policy § 7.1; OPM 2014 Policy § 7.1. There is nothing in these policies that specifies who, as between an agency and contractor, must provide notice, and there is nothing preventing a party required by state law to notify the victims of a data breach from doing so.

An OMB memorandum that KeyPoint quotes only in part to suggest it is insulated from responsibility for providing notice of data breaches actually suggests that contractors' "roles, responsibilities, and relationships" may figure in the notification policy and plan.

> When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* at 16 (May 22, 2007). KeyPoint's brief omits the second sentence. *See* KP Mot. at 31. Read in full, it is apparent that this informal guidance neither purports to preempt state law nor relieves federal contractors of their obligations thereunder.

The memo's second sentence is consistent with OPM's policy that "[p]ersonnel not associated with the official notification procedures should not notify or otherwise inform the affected Subject(s) of lost PII." KP Mot. at 31 (citing OPM 2012 Policy § 7.2 and OPM 2014 Policy § 7.2). Importantly, this policy does not define *which* personnel are "associated with the official notification procedures," or preclude a contractor from filling such a role. OPM 2012 Policy § 7.2; OPM 2014 Policy § 7.2.[29]

KeyPoint's preemption argument reads language into internal policies that is not there. These policies, in fact, set only minimum notification standards and permit contractors to have

[29] According to KeyPoint, "Plaintiffs admit that OPM—not KeyPoint—was responsible for alerting victims of the alleged KeyPoint cyber attack. Compl. ¶ 120." KP Mot. at 31. That is incorrect. The cited complaint paragraph simply alleges that "[o]n April 27, 2015, OPM alerted more than 48,000 federal employees that their personal information might have been exposed in the KeyPoint Breach." Compl. ¶ 120.

roles and responsibilities in notification procedures. The state data breach laws neither stand as an obstacle to, nor frustrate the purpose of, these federal materials.[30]

iii. Nothing in FISMA Conflicts with the Data Breach Acts.

FISMA also contemplates that federal contractors may exercise responsibilities in information security programs. The statute requires each agency to develop an information security program that both provides for the training of its contractors and includes "*their responsibilities* in complying with agency policies and procedures designed to reduce these risks." 44 U.S.C. § 3554(b)(4) (emphasis added). Section 3544(b) does not provide that any actor should or must disregard state data breach laws. Nor does FISMA require agencies to provide notice of data breaches or prohibit any party from providing notice to affected parties. There is no conflict here, and no conflict preemption.[31]

2. The Data Breach Acts Apply to KeyPoint's Conduct.

KeyPoint follows a strategy of narrowly interpreting state data breach notification laws that resembles its efforts to escape liability under state UDAP laws. First, KeyPoint relies on language in the Georgia, Kansas, Michigan, and Wisconsin data breach statutes to argue that these laws foreclose a private right of action. *See* KP Mot. at 32. The courts have, however,

---

[30] KeyPoint's preemption argument is also premature because facts relating to the dissemination, scope, and implementation of the OMB memorandum and OPM policies are not currently known. *See, e.g.*, *White v. Wachovia Bank, N.A.*, 563 F. Supp. 2d 1358, 1369 (N.D. Ga. 2008) (finding a preemption ruling premature in the absence of "record evidence"); *Lincoln-Dodge, Inc. v. Sullivan*, 588 F. Supp. 2d 224, 231 (D.R.I. 2008) (holding that a preemption issue "is not an 'unmixed question of law' but, rather, it is a mixed question of law and fact."); *Harvey's Casino v. Isenhour*, 724 N.W.2d 705, 708 (Iowa 2006) (preemption issues ordinarily "must be evaluated with the aid of a factual record" and "involve mixed questions").

[31] It is KeyPoint's interpretation that is inconsistent with the statute as a whole: section 3554(b) contemplates that "personnel, including contractors," may have "responsibilities in complying with agency policies and procedures." 44 U.S.C. § 3554(b)(4); *see Corley v. United States*, 556 U.S. 303, 314 (2009) (in construing a statute, courts seek to give effect to all of its provisions).

recognized a private right of action under these statutes, including in the data breach context, because the statutory language either (1) does not expressly forbid private enforcement, or (2) is sufficiently ambiguous to permit a private action. *See Target*, 66 F. Supp. 3d at 1169–70 (denying the defendant's motion to dismiss the plaintiffs' claims under the data breach statutes of Georgia, Kansas, Michigan, and Wisconsin).

Second, when a statute defines a term, that meeting controls—making it inappropriate to consult a dictionary. *Burgess v. United States*, 553 U.S. 124, 129–30 (2008); *see also United States v. Lettiere*, 640 F.3d 1271, 1275 (9th Cir. 2011) ("[C]larification is not necessary when a statute defines its own terms."). Regardless of what KeyPoint may have found in the dictionary, many of these data breach statutes define "consumers" broadly, as "individuals" or state "residents," without a commercial nexus, and some of these laws do not employ the term "consumer" at all.[32]

Third, KeyPoint argues in a footnote that it is exempt on the purported grounds that it did not violate federal law. *See* KP Mot. at 32 n.24. But Plaintiffs allege that KeyPoint violated the Privacy Act, which applied to KeyPoint by virtue of its contract with OPM. Compl. ¶¶ 122–24.

Fourth, while the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.* (the "CCRA"), defines the individuals it protects as "customers," the statute's language indicates

[32] *See* Ga. Code Ann. § 10-1-912(a) ("individuals" and "resident"); 815 Ill. Comp. Stat. Ann. 530/10(a) ("an Illinois resident"); Kan. Stat. Ann. § 50-7a02(a) ("affected Kansas resident[s]"); Mich. Comp. Laws Ann. § 445.72(1) ("residents of this state"); N.H. Rev. Stat. Ann. § 359-C:20(I)(a) ("the affected individuals"); N.C. Gen. Stat. Ann. § 75-65(a) ("residents of North Carolina"); Tenn. Code Ann. § 47-18-2107(b) ("any resident of Tennessee whose . . . personal information was . . . acquired by an unauthorized person"); Va. Code Ann. § 18.2-186.6(A) ("any resident of the Commonwealth"); Wash. Rev. Code Ann. § 19.255.010(1) ("any resident of this state whose personal information was . . . acquired by an unauthorized person"); Wis. Stat. Ann. § 134.98(b) ("an individual[]" and "the individual[]").

that it may afford relief to individuals who provided "personal information to a business for the purpose of . . . obtaining a service from the business." Cal. Civ. Code § 1798.80(c). In this case, Plaintiffs provided their information to KeyPoint for the purpose of obtaining a service—a background check—necessary for their employment or promotion. Hence, KeyPoint's challenges to the CCRA claim (*see* KP Mot. at 32–33 & n.28) should also be rejected.

3. Plaintiffs Adequately Allege That KeyPoint's Violations of the Data Breach Acts Injured Them.

KeyPoint distorts the complaint in asserting Plaintiffs have not alleged injury and causation under the state data breach statutes. KeyPoint erroneously states, for example, that Plaintiffs fail to allege that they received notice of the December 2013 KeyPoint Breach. *See* KP Mot. at 34. Plaintiffs in fact allege the specific notification dates for each breach: April 27, 2015 for the December 2013 KeyPoint Breach (Compl. ¶ 120); June 4, 2015 for the October 2014 OPM Breach (*id*. ¶ 138); and July 9, 2015 for the May 2014 OPM Breach (*id*. ¶ 140).

KeyPoint's characterization of Plaintiffs' alleged injuries as "conclusory" does not make them so. KP Mot. at 33. Rather, as the *Target* decision confirms, Plaintiffs' allegations have the requisite specificity. The plaintiffs in *Target* asserted injury based on the fact that they would not have shopped at Target had Target promptly notified them of the data breach pursuant to state data breach statutes. 66 F. Supp. 3d at 1166. Target argued that this alleged injury was not cognizable because it lacked specific details. *Id*. The court held that plaintiffs had adequately alleged injury, observing that if discovery showed Target should have learned about the breach immediately and provided notice shortly thereafter, "then nearly every putative class member may be able to claim 'would not have shopped' damages." *Id*.

Plaintiffs' short and plain statement that, had KeyPoint provided the prompt notice of the KeyPoint Breach that it was required by statute to provide, Plaintiffs would have avoided or

more effectively mitigated the ensuing harm, including by ordering account closures and credit freezes, is likewise adequate. Compl. ¶ 263. These allegations raise issues of fact, particularly when one considers the lengthy delay of several months, even after the KeyPoint Breach was discovered, in delivery of notice.[33] *Id*. ¶¶ 117, 120. As a result, KeyPoint's injury and causation arguments are, at best, "premature." *Target*, 66 F. Supp. 3d at 1166.

VIII. THE COMPLAINT STATES CLAIMS AGAINST OPM AND KEYPOINT FOR BREACH OF CONTRACT.

A. Plaintiffs Adequately Allege That OPM Breached Its Contract With Them.

Plaintiffs allege that OPM breached contractual obligations by failing to honor its promise to protect Plaintiffs' personal information in exchange for their providing it to OPM. Compl. ¶¶ 186–95. OPM bases its argument for dismissal upon the assumption that the Privacy Act, and nothing else, undergirds Plaintiffs' claim inasmuch as the government's Standard Forms reproduced the Privacy Act requirements. *See* OPM Mot. at 51–52. But the complaint alleges that it was in return for OPM's separate, express assurance that their "information will be protected from unauthorized disclosure"—and *not* the provisions of the Privacy Act—that Plaintiffs proffered their information. Compl. ¶¶ 190, 192. Plaintiffs further allege that OPM breached this contract by failing to protect their information, resulting in damages. *Id.* ¶ 193. Plaintiffs state a claim and properly invoke this Court's jurisdiction under the Little Tucker Act.

[33] In a footnote in its notification argument, KeyPoint cites *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014). *See* KP Mot. at 33 n.27. The ten-day delay in notification in *Sony Gaming* is different by an order of magnitude from the facts of this case. Plaintiffs allege far lengthier (and more consequential) delays, whether judged by delay in notification from breach occurrence or breach discovery. *See* Compl. ¶¶ 117, 120 (December 2013 KeyPoint Breach was detected in September 2014, but not disclosed until April 27, 2015). In another footnote, KeyPoint states—incorrectly—that Plaintiffs "do not allege that KeyPoint received any medical records." *Compare* KP Mot. at 34 n.28, *with* Compl. ¶ 144 (alleging Plaintiffs' "[p]sychological and emotional health information" was among the information compromised).

1. The Complaint Pleads the Breach of a Contract Between OPM and Plaintiffs.

"[A]ny agreement can be a contract within the meaning of the Tucker Act, provided that it meets the requirements for a contract with the Government, specifically: mutual intent to contract including an offer and acceptance, consideration, and a Government representative who had actual authority to bind the Government." *Massie v. United States*, 166 F.3d 1184, 1188 (Fed. Cir. 1999) (citation omitted). Under this standard, Plaintiffs allege facts sufficient to show the formation of a contract with OPM: namely, an offer by OPM that it would ensure any information submitted "will be protected from unauthorized disclosure" (Compl. ¶¶ 189–90); an acceptance by Plaintiffs when they submitted personal information (*id*. ¶ 190); an exchange of valuable consideration (*id*. ¶¶ 189–90); mutuality of intent to contract (*id*. ¶ 189–90); and actual authority to bind the government (*id*. ¶ 191). Plaintiffs also allege that OPM breached this express agreement by failing to protect Plaintiffs' data (*id.* ¶ 193), and that they suffered damages as a result (*id*. ¶ 194).

Plaintiffs allege, alternatively, that they entered into an implied-in-fact contract with OPM. Such a contract differs from an express contract "only in that it has not been committed to writing or stated orally in express terms, but rather is inferred from the conduct of the parties in the milieu in which they dealt." *Bloomgarden v. Coyer*, 479 F.2d 201, 208 (D.C. Cir. 1973). Offer and acceptance must "be manifested by conduct" that, viewed objectively, "indicates assent to the proposed bargain." *Russell Corp. v. United States*, 537 F.2d 474, 482 (Ct. Cl. 1976). Here, even apart from the specific promise in the Standard Forms, the course of conduct between the parties objectively evinces a tacit agreement under which OPM would take reasonable steps to protect Plaintiffs' personal information, and Plaintiffs manifestly indicated their assent to this proposed bargain by submitting their private information.

Data breach cases at both the circuit and district court levels bear out that Plaintiffs adequately allege the existence of a contract and a breach of that contract by OPM. In *Hannaford Brothers*, the Court of Appeals addressed a contract claim arising from the unauthorized use of plaintiffs' credit and debit card numbers after hackers breached the defendant's electronic payment system. 659 F.3d 151, 158–59 (1st Cir. 2011). The court found that "[w]hen a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. . . . [and] does not expect—and certainly does not intend—the merchant to allow unauthorized third parties to access that data." *Id*. at 159. Given the reasonable inferences from the facts alleged, "[a] jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract." *Id*.; *accord Irwin v. Jimmy John's Franchise, LLC*, No. 14-2275, --- F. Supp. 3d ----, 2016 WL 1355570, at *3 (C.D. Ill. Mar. 29, 2016) ("When the customer uses a credit card for a commercial transaction, he intends to provide the data to the merchant, and not to an unauthorized third party."); *Michaels Stores*, 830 F. Supp. 2d at 531–32 (finding the reasoning in *Hannaford Brothers* "persuasive"); *Target*, 66 F. Supp. 3d at 1176–77 (holding that whether the plaintiffs used their credit cards to purchase goods in exchange for the merchant agreeing to safeguard their personal and financial information, thereby creating an implied contract, presented a fact question for the jury); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864–65 (N.D. Cal. 2011) (upholding breach of contract claims where the plaintiff submitted his personal information to a web and app developer that failed to protect it).

Like the plaintiffs in *Hannaford Brothers* and the other cases cited above, Plaintiffs provided their personal information to OPM. The information was both more extensive and more sensitive than payment card numbers. Compl. ¶¶ 144, 190. And they turned over this

information to OPM in exchange for the promise that it would be kept safe and not improperly disclosed. *Id.* ¶ 190. Thus, they expected that OPM would take reasonable steps to protect their information from theft. *Id.* ¶ 192. No more is needed to show the creation of a binding contract.

OPM's legal arguments—"[t]hat which one is under a legal duty to do, cannot be the basis for a contractual promise" (OPM Mot. at 50 (citing *Floyd v. United States*, 26 Cl. Ct. 889, 891 (Cl. Ct. 1992))); and "[t]he violation of the statute or regulation will not be enforceable through a contract remedy" (OPM Mot. at 53 (citing *Pressman v. United States*, 33 Fed. Cl. 438, 444 (Fed. Cl. 1995)))—miss the mark. OPM's Standard Forms do not limit the protections to be afforded to those mandated by the Privacy Act:

> The information you provide is for the purpose of investigating you for a national security position, and the information will be protected from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information are governed by the Privacy Act.

OPM Mot. at 49. OPM italicizes only the second sentence, which states that the Privacy Act governs how the government will collect, maintain, and disclose Plaintiffs' information. But it is in the first sentence that OPM promised to "protect[]" Plaintiffs' information against "unauthorized disclosure." This promise stands by itself. It is not defined by reference to the Privacy Act. And it is this specific promise that gives rise to Plaintiffs' claim for breach of contract. Compl. ¶¶ 190, 192. It is thus not a violation of a statute or regulation, as in *Pressman*, 33 Fed. Cl. at 444, or a violation of employment regulations as in *Army & Air Force Exchange Service v. Sheehan*, 456 U.S. 728 (1982), but a breach of a distinct contractual promise to protect their data, upon which Plaintiffs' claim is founded. Compl. ¶¶ 192–93.[34]

[34] *Tripp v. United States* also throws the facts here into relief: Ms. Tripp did not "point[] the Court to an express or implied contract" but "relie[d] only on the 'binding and specific' regulations governing the [Department of Defense]'s release of information contained in a

[Footnote continued on next page….]

2. Plaintiffs' Claims for Breach of Contract Satisfy the Jurisdictional Requirements of the Little Tucker Act.

By alleging that OPM breached its contract with them, Plaintiffs properly invoke the Court's jurisdiction under the Little Tucker Act. 28 U.S.C. § 1346(a)(2).[35] In arguing that no governmental waiver of sovereign immunity has been established under the Little Tucker Act, OPM claims that a contract must expressly provide for the payment of money to be cognizable under the Act. *See* OPM Mot. at 52–54. In fact, "when referencing the money-mandating inquiry for Tucker Act jurisdiction, the cases logically put to one side contract-based claims" because the normal remedy for breach of contract is money damages. *Holmes v. United States*, 657 F.3d 1303, 1314 (Fed. Cir. 2011); *see also Sanders v. United States*, 252 F.3d 1329, 1334 (Fed. Cir. 2001) (same).

A plurality of the Supreme Court in *United States v. Winstar Corporation* held that the Tucker Act does not require that the contract expressly provide for money damages, chastising the dissent for going

> so far as to argue that our conclusion that damages are available for breach even where the parties did not specify a remedy in the contract depends upon "reading of additional terms into the contract." That, of course, is not the law; damages are always the default remedy for breach of contract. And we suspect that most Government contractors would be quite surprised by the dissent's conclusion that, where they have failed to require an express provision that damages will be available for breach, that remedy must be "implied in law" and therefore unavailable under the Tucker Act.

518 U.S. 839, 885–86 (1996) (plurality opinion) (citations omitted).

Privacy Act 'system of records' as the source of defendant's alleged contractual obligations to her." 257 F. Supp. 2d 37, 47 (D.D.C. 2003).

[35] The Little Tucker Act vests the district courts, along with the federal court of claims, with jurisdiction over claims "against the United States, not exceeding $10,000 in amount, founded . . . upon any express or implied contract with the United States . . . ." 28 U.S.C. § 1346(a)(2).

"Put another way, in a contract case, the money-mandating requirement for Tucker Act jurisdiction normally is satisfied by the presumption that money damages are available for breach of contract, with no further inquiry being necessary." *Holmes*, 657 F.3d at 1314. OPM's argument, like the position of the dissent in *Winstar*, "is not the law." 518 U.S. at 885.

B. Plaintiffs Adequately Allege That KeyPoint Breached a Unilateral Contract.

Plaintiffs allege that KeyPoint "offered to ensure the confidentiality of Plaintiffs' and Class members' GII in exchange for their submission of information needed to conduct background and security investigations" (Compl. ¶¶ 269–70), and that Plaintiffs accepted this offer, entering into a unilateral contract with KeyPoint "by permitting KeyPoint to access their sensitive personal information" (*id.* ¶ 271). KeyPoint's Privacy Policy stated that KeyPoint would protect the information Plaintiffs submitted for background and security check purposes from unauthorized disclosure. *Id.* ¶ 77. KeyPoint violated that policy, and breached its contract, by failing to establish appropriate data security safeguards, leaving its network vulnerable to cyberattacks (*id*. ¶¶ 117, 121–22, 274) and thereby exposing Plaintiffs' information to hackers and causing Plaintiffs to incur damages (*id*. ¶¶ 13–50, 275).

KeyPoint's casual rejection of Plaintiffs' breach of contract claim, on the grounds that "Plaintiffs fail to allege any written contract," overlooks that with "a unilateral contract, performance constitutes acceptance of an offer." *United States ex rel. Modern Elec. v. Ideal Elec. Sec. Co.*, 81 F.3d 240, 244 (D.C. Cir. 1996) (citation omitted). "This principle is well-recognized, even outside District of Columbia common law." *Id.*; *see also City of Houston v. Williams*, 353 S.W.3d 128, 136 (Tex. 2011) ("We have explained that '[a] unilateral contract occurs when there is only one promisor and the other accepts . . . by actual performance,' rather than by the usual mutual promises.") (citations omitted). "An offer for a unilateral contract

generally requires an act on part of the offeree to make a binding contract. This act is consideration for the promise contained in the offer and doing it with intent to accept without more will create a contract." 1 Williston on Contracts § 65 (3d ed.).

A written offer inheres in KeyPoint's Privacy Policy, which promises that KeyPoint "safeguards confidential consumer information from unauthorized internal and external disclosure, by maintaining a secure network, limiting access to KeyPoint's computer terminals and files, and maintaining backup data in encrypted form." Compl. ¶ 77. Plaintiffs' act of granting KeyPoint access to their personal information was both consideration for and acceptance of the offer made by KeyPoint in its Privacy Policy. *Id*. ¶¶ 269–73.[36]

KeyPoint's efforts to downplay and, indeed, to ignore, its Privacy Policy as the contractual predicate fail categorically, for the courts have found that performance undertaken in reliance on such a privacy policy gives rise to a unilateral contract. Three cases are especially noteworthy. In *Meyer v. Christie*, where the court allowed a breach of contract claim to proceed, the court rejected the defendant's "attempt to characterize its privacy policy as nothing more than a mere unilateral statement of company policy," concluding that the plaintiff had "divulged information to the bank with the understanding that the bank would keep it confidential in accordance with its privacy policy." No. 07-2230-JWL, 2007 WL 3120695, at *4 (D. Kan. Oct. 24, 2007). In the *In re Jetblue Airways Corporation Privacy Litigation*, the court upheld the plaintiffs' allegations "that a stand-alone contract was formed at the moment they made flight

[36] KeyPoint's argument that the allegations could be more detailed (*see* KP Mot. at 44) holds the complaint to a standard higher than the liberal notice pleading Plaintiffs are required to satisfy. *See Jefferson v. Collins*, 905 F. Supp. 2d 269, 278 (D.D.C. 2012) (applying notice pleading standards to contract claim); *Smith v. Wash. Post Co.*, 962 F. Supp. 2d 79, 87–88 (D.D.C. 2013) (same). Plaintiffs' allegations are sufficient to place KeyPoint on notice of their claim for relief.

reservations in reliance on express promises contained in [defendant's] privacy policy." 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005). And most recently, the court in *Enslin v. The Coca-Cola Company* allowed a breach of contract claim to proceed where the defendant, "through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard [plaintiff's data] in exchange for his employment." 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015).

CONCLUSION

For all the foregoing reasons, Defendants' motions to dismiss should be denied. Should the Court find the complaint inadequate in any respect, Plaintiffs respectfully request permission to amend. Fed. R. Civ. P. 15(a)(2); *Firestone v. Firestone*, 76 F.3d 1205, 1209 (D.C. Cir. 1996).

DATED: June 30, 2016

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Daniel C. Girard*
Daniel C. Girard

Jordan Elias
Esfand Y. Nafisi
Linh G. Vuong
601 California Street, 14th Floor
San Francisco, CA 94108
(415) 981-4800
dcg@girardgibbs.com

Interim Lead Class Counsel

David H. Thompson
Howard C. Nielson, Jr.
Peter A. Patterson
Harold Reeves
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
Theodore Maya
Bradley King
Vanessa T. Shakib
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
Marcio W. Valladares
Patrick A. Barthle II
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
Ben Branda
WHITFIELD BRYSON & MASON LLP
1625 Massachusetts Avenue, N.W., Suite 605
Washington, D.C. 20036

Liaison Counsel

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
Lindsay Todd Perkins
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112

Steven W. Teppler
ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223

Denis F. Sheils
KOHN, SWIFT & GRAF, P.C.
One South Broad Street, Suite 2100
Philadelphia, PA 19107

Mark R. Rosen
Chad A. Carder
BARRACK, RODOS & BACINE
Two Commerce Square
2001 Market Street, Suite 3300
Philadelphia, PA 19103

Plaintiffs' Counsel on the Brief