NOT YET SCHEDULED FOR ORAL ARGUMENT

No. 19-7020

UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

CHANTAL ATTIAS, Individually and on behalf of all others similarly situated, *et al.*

Plaintiffs - Appellants,

v.

CAREFIRST, INC., *et al.,*

Defendants - Appellees.

On Appeal from the United States District Court for the District of Columbia, in Case No. 1:15-cv-882 (CRC), Christopher R. Cooper, Judge

REPLY BRIEF OF APPELLANTS

Troy N. Giatras, Esq.
Bar Number: 429086
THE GIATRAS LAW FIRM, PLLC
118 Capitol St., Ste. 400
Charleston, WV 25301
Phone: 304.343.2900
troy@thewvlawfirm.com
Counsel for Appellants

Christopher T. Nace, Esq.
Bar Number 54503
PAULSON & NACE, PLLC
1025 Thomas Jefferson St. NW
Suite 810
Washington, D.C. 20007
Phone: 202.463.1999
ctnace@paulsonandnace.com
Counsel for Appellants

Jonathan B. Nace, Esq.
Bar Number 60148
NIDEL & NACE, PLLC
2201 Wisconsin Ave.NW
Suite 200
Washington, D.C. 20007
Phone: 202.780.5153
jon@nidellaw.com
Counsel for Appellants

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES ii

SUMMARY ARGUMENT 1

ARGUMENT 1

1. This Court recently Decided the Issue of Actual Damages in *OPM*. 1

2. The Inclusion of More Named Plaintiffs does not Increase the Adequacy of a Complaint. 7

3. The Plaintiffs Have Pled Actual Misuse of Personal Information. 8

4. Appellants Clearly Pled Breach of Contract under DC Law 9

5. This Court has Espoused its Position on Mitigation Costs in *OPM*. 11

6. The Plaintiffs have Adquately Pled Emotional Distress as Actual Damages as Part of an Invasion of Privacy Claim. 12

7. The Recognition of a Duty in Tort is the Purview of the Courts. 14

8. The District Court Continues to Read Choharis Over Broadly and Appellants are Entitled to Plead in the Alternative. 17

CONCLUSION 19

RULE 32 CERTIFICATION. 21

CERTIFICATE OF SERVICE 22

ADDENDUM: CONSOLIDATED AMENDED COMPLAINT A1

TABLE OF AUTHORITIES

Cases ***Page(s)***

Attias v. Carefirst, Inc.,
865 F.3d 620 (D.C. Cir. 2017),
cert. denied, 138 S.Ct. 981,
200 L.Ed. 2d 248 (2018) 5

Capital Keys, LLC v. Democratic Republic of Congo,
278 F.Supp.3d 265, 272 (D.D.C. 2017) citing *Id.*
United House of Prayer for All People v. Therrien Waddell, Inc.,
112 A.3d 330, 339-40 (D.C. 2015) 10

Choharis v. State Farm Fire & Casualty,
961 A.2d, at 1088 (D.C. 2008).....17, 18

Colonial Penn Ins. Co. v. Coil,
887 F.2d 1236, 1239 (4th Cir. 1989) 4

Dittman v. UPMC,
196 A.3d 1036, 1046 (Pa. 2018).....14

Doe v. Dominion Bank of Washington,
963 F.2d 1552 (1992).....15

G-I Holdings, Inc. v. Baron & Budd,
238 F. Supp. 2d 521, 534 (S.D.N.Y. 2002) 18

Graham v. M & J Corp.,
424 A.2d 103, 105 (D.C. 1980) 16

In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.,
928 F. 3d 42 (D.C. Cir. 2019).....1, 2, 3, 4, 5, 12, 16

In re U.S. Office of Personnel Management Data Security Breach Litigation,
WL 11218210 (D.D.C.) 4

Kline v. 1500 Massachusetts Ave. Apartment Corp.,
439 F.2d 477, 482-83 (D.C. Cir. 1970).....15

Randolph v. ING Life Ins. & Annuity Co.,
973 A.2d 702 (D.C. 2009) 7, 8, 11

Remijas v. Neiman Marcus Grp.,
794 F.3d 688 (7th Cir. 2015).....5

Smith v. Duncan,
297 F.3d 809, 815 (9th Cir. 2002) 4

U.S. ex rel Landis v. Tailwind Sports Corp.,
234 F.Supp.3d 180, 199 (D.D.C. 2017)
quoting *United States v. Bornstein*,
423 U.S. 303, 324, n. 13, 96 S.Ct. 523,
46 L.Ed.2d 514 (1976)(Cooper, J.) 10

Vassiliades v. Garfinckel's, Brooks Bros.,
492 A.2d 580, 594 (DC 1985) 13

Vector Realty Group v. 711 14TH STREET,
659 A.2d 230, 234 (D.C. 1994) 9

White v. Gaetz,
588 F.3d 1135, 1137 n. 2 (7th Cir. 2009) 4

*Workman v. United Methodist Comm. on Relief of Gen.
Bd. of Glob. Ministries of United Methodist Church*,
320 F.3d 259, 265 (D.C. Cir. 2003).....16

Statutes

Privacy Act, 5 U.S.C. § 552a(g)(1)(D).....2
Federal Rules of Civil Procedure 10(e)(c)(2) 4
Federal Rules of Civil Procedure 10(e)(2)(a) 4
Federal Rule of Civil Procedure 12(b)(1).....8
Federal Rule of Civil Procedure 12(b)(6).....1, 6, 7, 8, 16, 20
Federal Rule of Evidence 201.....4
REINSTATEMENT (SECOND) OF CONTRACTS § 347
comment (1981) 10

SUMMARY ARGUMENT

In their Complaint, Plaintiffs-Appellants pled damages in the form of economic and noneconomic harm, including mitigation damages, the loss of the benefit of their bargain, time spent addressing the data breach, and other harm. The issue before this Court, then, is whether Plaintiffs, victims of a data breach which exposed sensitive personal and financial information, sufficiently pled damages at the Rule 12(b)(6) stage. Appellee relies entirely and exclusively on the lower court's opinion that Plaintiffs failed to plead actual damages. Plaintiffs-Appellants respectfully request that this Court reverse the district court's decision, and remand the case because they sufficiently pled damages.

ARGUMENT

1. This Court Recently Decided the Issue of Actual Damages in OPM.

On June 21, 2019, this Court handed down its opinion in *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42 (D.C. Cir. 2019).[1] In *OPM*, the D.C. Circuit considered whether the plaintiffs in that case sufficiently pled actual damages. *Id.* This Court reversed the lower court's order, in relevant portion, and explicitly held that the plaintiffs had in fact sufficiently pled damage. *Id.* at 66.

[1] The *OPM* Opinion issued one day before Appellants' opening brief was due. *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42 (D.C. Cir. 2019).

Appellees argue that *OPM* is distinguishable because it involved allegations of the violation of the Privacy Act. 5 U.S.C. § 552a(g)(1)(D). Contrary to Appellee's assertion, the Privacy Act is actually more stringent with regard to damages than most torts, limiting "actual damages" to *proven* pecuniary or economic harm. Appellees admit that, per *OPM*, the costs of credit monitoring are actual damages. *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 61 (D.C. Cir. 2019)(Finding that Plaintiffs "… can redress certain proven injuries related to that risk (such as reasonably-incurred credit monitoring costs)").

Despite acknowledging that cost of credit monitoring is an actual damage, Appellee still argued that some members of the class in that case merely purchased credit protection and/or credit repair services after learning of the breach. Brief of Appellee, ("Response Brief") p.21. This is contradictory to Appellee's argument that the *OPM* Court only found actual damages to have been alleged regarding expenses incurred to combat "*actual misuse that had already allegedly occurred*." *Id*. This is not accurate. In fact, one of the *OPM* plaintiffs' subscription to monthly credit monitoring service was deemed by the *OPM* Court to be "the paradigmatic example of 'actual damages' resulting from the violation of privacy protections." *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 65 (D.C. Cir. 2019).

Indeed, even time spent with no out-of-pocket loss alleged qualified as actual damages in OPM. *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 66 (D.C. Cir. 2019). This Court allowed the entire class to move forward in *OPM* based upon the pleadings. The *OPM* complaint shares many similarities with the Appellants' in this case, and specifically pleads damages in the form of time spent dealing with the data breach. As an example, the *OPM* Complaint includes the following named plaintiffs:

> 15. Plaintiff Ryan Bonner resides and is domiciled in the state of Pennsylvania. He formerly worked at the Transportation Security Administration, as a Transportation Security Officer. Bonner provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. **His exposure to the Data Breaches has caused Bonner to review his credit reports and financial accounts with greater frequency.**
>
> 33. Plaintiff Jennifer Gum resides and is domiciled in the state of Kansas. She works as a Medical Reimbursement Technician for the Veterans Affairs Medical Center, and her Case 1:15-mc-01394-ABJ Document 63 Filed 03/14/16 Page 16 of 77 17 husband works as a Senior Corrections Officer with the Federal Bureau of Prisons. She began working for the Department of Veterans Affairs in 2011. Gum and her husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. **Her exposure to the Data Breaches has caused Gum to review her financial accounts with greater frequency.**
>
> 40. Plaintiff Teresa J. McGarry resides and is domiciled in the state of Florida. She currently works in the Social Security Administration as an Administrative Law Judge. McGarry previously served as an Assistant United States Attorney and as a Judge Advocate General with the Navy. McGarry provided sensitive personal information to

> the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. **McGarry thereafter purchased a monthly subscription for credit and identity monitoring. Her exposure to the Data Breaches has also caused McGarry to review her financial accounts with greater frequency.**
>
> 47. Plaintiff Darren Strickland resides and is domiciled in the state of North Carolina. Strickland worked for many years for federal government contractors. Strickland provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. **His exposure to the Data Breaches has caused Strickland to review his financial accounts with greater frequency.**

In Re: U.S. Office of Personnel Management Data Security Breach Litigation, 2016 WL 11218210 (D.D.C.) (emphasis added).[2]

The district court in the *OPM* case dismissed plaintiffs' claims (members of the so-called "Arnold" plaintiffs), and this Court disagreed. This is notable because

[2] Appellants request that pursuant Federal Rule of Appellate Procedure 10(e)(c)(2) and Federal Rule of Evidence 201 that the pleading filed in *OPM* be considered in this pending appeal. OPM was handed down a day before Appellant filed the opening brief and the parties already reached an agreement regarding the appendix making it virtually impossible to have included this document in the original appendix. This Court recently found the OPM pleading adequate and it is an incontrovertible public document that would assist in evaluating the instant appeal. *White v. Gaetz*, 588 F.3d 1135, 1137 n. 2 (7th Cir. 2009) (taking judicial notice on appeal of state court transcript); *Smith v. Duncan*, 297 F.3d 809, 815 (9th Cir. 2002) (taking judicial notice of the tolling period based on documents in state case that had a direct relationship to federal habeas appeal); *Colonial Penn Ins. Co. v. Coil*, 887 F.2d 1236, 1239 (4th Cir. 1989) (taking judicial notice of appellees' guilty pleas in separate proceedings because they "are most relevant and critical," involving "the very property and issues involved in this proceeding"). In the meantime, undersigned counsel will seek a stipulation from Appellee pursuant to FRAP 10(e)(2)(a) to address this issue.

the only damages these listed plaintiffs (*inter alia*) alleged was their time and effort spent resulting from the data breach, and the stress and concern attendant therefrom. The Court was, of course, free to rule that only those which it examined in its opinion survived the motion to dismiss, and dismiss all others. It did not. Instead, this Court allowed all of the plaintiffs' claims to survive the motion to dismiss.

This Court had occasion to analyze its own decision in *this* case when deciding *OPM*.[3] In *OPM*, the district court largely disregarded this Court's previous opinion in this case, reasoning that the *OPM* plaintiffs still did not have standing because the type of damages alleged (that is, the type of information stolen, and by whom), was much more clearly damaging here than in the *OPM* data breach. The district court in *OPM* held that:

> The *Attias* Court based its decision on a particular cybercrime in a commercial setting—"the hack and the nature of the data that the plaintiffs allege was taken"—and it did not purport to address every data breach, including those that might be state-sponsored. Since the Court lacks the basis available in *Remijas* or *Attias* to "presume" that the purpose of this hack was to facilitate fraud or identity theft, this case is more analogous to *Clapper*, and it is not plausible to infer that plaintiffs now face a substantial risk of identity theft based on the allegations in the complaint.

In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 35 (D.D.C. 2017), aff'd in part, rev'd in part and remanded, 928 F.3d 42 (D.C. Cir. 2019).

[3] Admittedly, this appeared in the analysis regarding standing, but is still relevant.

This Circuit Court reversed that decision. While that analysis involved standing, it is instructive because the damages alleged in this case may be considered more significant than those alleged in *OPM.* And in *OPM* **this Court allowed each claim to survive a Rule 12(b)(6) challenge**.

The *OPM* Complaint, which survived 12(b)(6) scrutiny also listed as common to all class members damages in the form of "money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of [sensitive personal data], including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards" as well as "continuing risks from the unmasking of confidential identities." *OPM* Complaint, ¶ 163. Appellants in this case alleged substantially the same damages in their Complaint:

> 19. Consequently, the Plaintiffs and Class Members have or will have to spend significant time and money to protect themselves; **including, but not limited to: the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, cost of conducting a damage assessment, mitigation costs, costs to rehabilitate Plaintiffs' and Class Members' PII/PHI/Sensitive Information, and costs to reimburse from losses incurred as a proximate result of the breach.**

Appellant's Second Amended Complaint (App. pp. 20-21).

In both cases the alleged damages are the same: individuals who have had their data stolen owing to a company's failure to safeguard that data must spend

time and money which they otherwise would not have spent dealing with the loss of that information.

2. The Inclusion of More Named Plaintiffs does not Increase the Adequacy of a Complaint.

Appellee bases the majority of its attempt to distinguish *OPM* from the instant case on the fact that, in *OPM*, more named plaintiffs were listed and described. This flawed reasoning completely disregards the very purpose of class actions. Never has it been a requirement – at the pleading stage or otherwise – that named plaintiffs be included or described in a class action complaint. In the instant case, fewer individuals are named and described in the Appellant's Complaint, but all of those individuals have pled claims and damages which are the same or *more* specific than many of the claims in *OPM*, which this Court unequivocally decided passed 12(b)(6) scrutiny.

The lower court, without the benefit of this Court's recent opinion in *OPM* wrongfully relied upon another standing case, *Randolph*, which used the plaintiffs' *likely* failure to state a claim in order to find a lack of standing. *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708 (D.C. 2009). In its response, Appellee asserts that Appellants failed to recognize that the outmoded decision in *Randolph* did, in fact, analyze the plaintiffs' damage allegations in order to find that they did not have standing. In fact, the Appellants, themselves, pointed this out to the Court, reasoning that the Court, in so finding out-of-hand that the Appellants in this case

had Article III standing to bring this class action lawsuit, if it were to follow the same analysis as it did in *Randolph*, this Court clearly would have found damages to be adequately alleged. *See* Appellant's Appeal Brief, pp. 25-26.

3. The Appellants Have Pled Actual Misuse of Personal Information.

In its Response, Appellee makes much of the amount of time which has passed since the breach occurred. Response, at 14. As discovery has not yet begun, the full extent of the harm visited upon Appellants and the potential class members is not yet known. The length of time which has passed between the Appellee's blunder and the present date is entirely irrelevant.

Regardless, Appellee's position that substantial threat of misuse of personal information does not constitute damage is a) not supported by authority, and b) immaterial, since the Appellants have adequately pled *actual* misuse of personal information. First, the Appellee's primary "authority" for its position is the district court's opinion *in this very case*. This is the very opinion being challenged by Appellants.[4] The only other authority presented is this Court's opinion in *Randolph*, a standing case, which, as discussed, used a 12(b)(6) analysis to decide a 12(b)(1) issue in the negative.

[4] This tautological approach to "authority," in fact, is a running theme throughout the response, and should be noted and its arguments disregarded each time it is presented.

More importantly, the Appellee's point is belied by the fact that the Appellants have plead actual misuse of personal information:

> 17. The Plaintiffs and Class Members now face an increased risk of identity theft, **and also actual identity theft and resulting losses**, and need to take immediate action to protect themselves from identity theft, which have already and will continue to result in real and actual loss regardless of whether identity theft actually occurs.

Appellant's Second Amended Complaint (App. 20).

Even were this Court to find that the threat of misuse of personal information is insufficient to qualify as actual damages, the fact is that, at this procedural stage, Appellants have adequately pled actual misuse of personal information.

4. Appellants Clearly Pled Breach of Contract under DC Law.

Appellee curiously states that Appellants did not allege a breach of contract claim under DC law. This is clearly false, and is in fact contained in Count I, ¶¶ 64-75 of the Second Amended Complaint (App. 33-34). Regardless, Appellee again uses the lower court's opinion to justify the lower court's opinion that Appellants clear loss of the benefit of their bargain with the Appellee somehow does not qualify as actual damages.

A loss of the benefit-of-the-bargain is an actual damage, which this Court has recognized. For instance, in *Vector Realty Group v. 711 14TH STREET*, 659 A.2d 230, 234 (D.C. 1994), this Court found that:

> Contract damages ... are intended to give the injured party the benefit of his bargain by awarding him a sum of money that will, to the extent possible, put him in as good a position as he would have been in had the contract been performed.

Id. (quoting RESTATEMENT (SECOND) OF CONTRACTS § 347 comment (1981)). Furthermore, "[u]nder District of Columbia law, the standard measure of actual damages arising from a breach of contract is the non-breaching party's expectation interest — that is, an amount sufficient to give the non-breaching party the benefit of the bargain." *Capital Keys, LLC v. Democratic Republic of Congo*, 278 F.Supp.3d 265, 272 (D.D.C. 2017) (Jackson, J.) (citing *Id.*; *United House of Prayer for All People v. Therrien Waddell, Inc.*, 112 A.3d 330, 339-40 (D.C. 2015)). *See also U.S. ex rel Landis v. Tailwind Sports Corp.*, 234 F.Supp.3d 180, 199 (D.D.C. 2017) (quoting *United States v. Bornstein*, 423 U.S. 303, 324, n. 13, 96 S.Ct. 523, 46 L.Ed.2d 514 (1976)) (Cooper, J.) (discussing False Claims Act damages and stating such "are generally measured on the 'benefit of the bargain' received by both parties. Under this approach, 'the government's actual damages are equal to the difference between the market value of the [products] it received and retained and the market value that the [products] would have had if they had been the specified quality.").

It is clear that the lower court disregarded a great deal of this Court's caselaw to go out of its way to use standing cases in order to find benefit of the bargain as not an "actual" damage.

Appellants pled damages in this form in several places:

> 21. Plaintiffs contracted for services that included a guarantee by Defendants to safeguard their personal information and, instead, ***Plaintiffs received services devoid of these very important protections.*** Accordingly, Plaintiffs allege claims for breach of contract, unlawful trade practices, unjust enrichment, negligence, and negligence per se.
>
> 73. Furthermore, Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs that were of a diminished value.

(App 21, 34). (emphasis added).

Therefore, Appellants have legally cognizable actual damages in the form of the loss of the benefit of their bargain with the Appellee.

5. This Court Has Espoused its Position on Mitigation Costs in *OPM*.

As discussed in Section 1, *supra*, this Court's opinion in *OPM* is dispositive on the issue as to whether mitigation costs qualify as actual damages. They do. When this Court overturned the district court in *OPM*, it clearly allowed through multiple claims of named plaintiffs in which the specific damages pled involved time and money spent on monitoring bank accounts and other sensitive reports for criminal or otherwise wrongful activity.

As is its theme throughout, Appellee relies upon the lower court's opinion (and, by extension, the standing case of *Randolph*), to convince this Court to accept the lower court's opinion. In addition, the Appellee points to myriad out-of-

circuit *district* court opinions for authority. Response at p. 15. This is all unnecessary, as *OPM* stands on all fours on this issue.

The *OPM* Court stated unequivocally that mitigation costs are "the paradigmatic example of 'actual damages' resulting from the violation of privacy protections." And, as stated, *supra*, even a plaintiff's time spent – with no out-of-pocket loss alleged save a decision to take time off work – qualified as actual damages. *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 66 (D.C. Cir. 2019).

6. The Appellants Have Adequately Pled Emotional Distress as Actual Damages as Part of an Invasion of Privacy Claim.

Appellee, again relying primarily on the very opinion which is at issue, fails to recognize that Appellants have adequately and sufficiently pled invasion of privacy claims, and, therefore, cases in which negligent infliction of emotional distress claims were dismissed are distinguishable and largely irrelevant. *See* Response Brief, at pp. 24-25.

Appellants' emotional distress claims are tied to the Appellee's breach of the duty of confidentiality. "A plaintiff whose private life is given publicity may recover damages…for the 'emotional distress or personal humiliation . . . if it is of a kind that normally results from such an invasion and it is normal and reasonable in its extent.' Actual harm need not be based on pecuniary loss, and emotional distress may be shown simply by the plaintiff's testimony. Proof of special

damages is not required." *Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580, 594 (D.C. 1985) (adopting the tort of breach of the duty of confidentiality and acknowledging non-economic damages are legally allowable under a theory for invasion of privacy and finding.). Appellee is incorrect that the operative complaint in this case does not allege intentional conduct which invaded Appellants' privacy. Appellants' Second Amended Complaint states:

> 118. **Defendants made false representations of material facts to Plaintiffs and members of The Class** in that Defendants proffered an Internet Privacy Policy and General Privacy Policy which indicated that information provided by Plaintiffs and members of The Class would be encrypted. Defendants further made false representations by claiming they would use various industry technologies to prevent unauthorized access of Plaintiffs' and members of The Class' personal information.
>
> 119. **Defendants made these false representations knowing them to be untrue and with reckless indifference for the truth**.
>
> 120. **The Defendants made these representations for the purpose of defrauding Plaintiffs and members of The Class** by inducing them to purchase Defendants' services and to use Defendants' online services.

Second Amended Complaint (App. 42-43). (emphasis added).

Again, Appellee's argument misstates the law of this Circuit, and any reliance on such misstatements made by the lower court was in error.

7. The Recognition of a Duty in Tort is the Purview of the Courts.

Even the lower court in this case acknowledged its power – and, by extension, the power of all courts in this Country – to recognize novel[5] duties exist in tort law. District Court Opinion, (App. 33, at 22). Even though the district court in this case declined to find that a duty exists to safeguard personal and confidential information, the lower court's *entire* analysis is rooted in caselaw discussing other courts' either permittance or refusal to do so. *Id.* In fact, the lower court **specifically called upon this Court to decide whether such a duty exists**. The district court stated:

> **Because the District of Columbia Court of Appeals has not determined one way or the other whether there is a common law duty to safeguard data**, the Court will follow the approach taken in some of the cases cited above and look to analogous case law regarding the nature of the relationship between insurers and insureds.

Id., at 23. (emphasis added).

Appellee finishes its analysis arguing against a simple duty to exercise due care with consumer data by pointing out that Appellants' appeal to this Court to

[5] "Novel" is perhaps a misnomer. The lower court even briefly discussed *Dittman v. UPMC*, 196 A.3d 1036, 1046 (Pa. 2018), in which the Supreme Court for the Commonwealth of Pennsylvania stated: "we agree with Employees that this case **is one involving application of an existing duty to a novel factual scenario, as opposed to the imposition of a new, affirmative duty requiring analysis of the** [case discussing finding legal duties] **factors**." *Id.* (emphasis added). In *Dittman*, the court found very wisely extended the duty to protect sensitive information in the duty to exercise reasonable care.

explicitly recognizing such duty "rel[ies] on authority from jurisdictions *outside* D.C." Response Brief at 29. (emphasis in original).

This Court has applied an independent duty of protection in other contexts in the past, including the duty to protect against criminal activity. In *Doe v. Dominion Bank of Washington*, 963 F.2d 1552 (1992), this Court stated that, because a landlord "was in a better position both to know about security threats and to protect against them." *Id.* at 1559. The Court relied upon the "inability of an individual tenant to control the security of common hallways, elevators, stairwells, and lobbies." *Id.* Other types of associations have similarly been held to be special such that a duty to protect is aroused. *See, e.g., Kline v. 1500 Massachusetts Ave. Apartment Corp.*, 439 F.2d 477, 482-83 (D.C. Cir. 1970).

Again, this is an entirely and completely logical extension in reasoning to the current situations facing the world of cybercrime. Customers simply are not the masters of their sensitive information once that information is surrendered in order to *buy health insurance*. It is apparent that, as consumers required to entrust to the Appellee myriad sensitive data, the Appellants had a special relationship[6] with the Appellee and were owed a duty from the Appellee to safeguard that data.

[6] As this point has been made *ad nauseum*, including in the Appellee's Response, the special relationship which exists to create the special duty is that of business-patron, which is explicitly recognized as such a relationship to give rise to a duty to protect against criminal activity. *See Kline v. 1500 Massachusetts Ave. Apartment Corp.*, 439 F.2d 477, 482-83 (D.C. Cir. 1970). Regarding the "special relationship"

Appellee points out that foreseeability is an issue, which the Appellants already addressed by noting that this Circuit has traditionally employed a foreseeability analysis, when such analysis is typically devoted to deciding whether the breach of a legally accepted duty was the proximate cause of injury. *See Workman v. United Methodist Comm. on Relief of Gen. Bd. of Glob. Ministries of United Methodist Church*, 320 F.3d 259, 265 (D.C. Cir. 2003). However, the Court has also stated that the foreseeability of the "criminal activity which caused the injuries…is a question of fact." *Graham v. M & J Corp.*, 424 A.2d 103, 105 (D.C. 1980). It stands to reason, then, that, even were this Court disinclined to recognize a blanket duty of businesses that trade in consumer information to protect that information, the Court's precedent still holds that dismissal – at least at the pleading stage – for want of such duty is always inappropriate as fact-intensive.

The Appellee, and companies like it, make money off of consumer data. It is not the earth-shattering policy shift the Appellee pretends it is to simply recognize a duty to exercise the duty of care in protecting individuals' data.

---

exception to the economic loss rule, explicit recognition of a duty of companies who trade in consumer data to safeguard that data would render the distinction moot, and this Court, in *OPM*, has already suggested its position regarding the economic loss doctrine when it allowed claims to survive a Rule 12(b)(6) motion to dismiss which only pled stress from the breach as damages. *See*, e.g., OPM Complaint, ¶ 35; *See also*, *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, at 66.

8. The District Court Continues to Read *Choharis* Over Broadly and Appellants are Entitled to Plead in the Alternative.

The district court, and, of course, Appellee, asserts that Appellants have failed to allege any facts which do not arise out of the contractual relationship. This is not true. The lower court utilizes Appellants' argument that it has done so *and also* pled breach of contract as a supposition that *Choharis* bars all tort claims.

Throughout its brief, Appellee continues its tired arguments that, for example: a) Appellees cannot plead both breach of contract and unjust enrichment (Response Brief, pp. 42-43); b) Appellants cannot plead violations of the DCCPA because it is duplicative of their breach of contract claim (*Id.*, pp. 39-41); and c) again, and *ad nauseum*, Appellants cannot plead *any* tort along with a breach of contract claim (Response Brief, pp. 30-33). Both the lower court and, of course, Appellee, fail to recognize Appellants' right to plead in the alternative.[7]

First, the district court misinterpreted the application of *Coharis* with regards to the claims of fraud and negligent misrepresentation. Clearly, this Court did not intend *any* contractual relationship to bar tort claims against a party insurer. It stated so clearly when it said:

> Choharis asserts that the consequence of the ruling by the trial court insulates insurance companies from any tort liability in the handling of policy claims made by their insureds. Such an interpretation goes

[7] This very well may be because, as the Appellee has managed to obstruct progress of this case for more than four (4) years, it seems implausible that it could still be at the pleading stage of litigation. However, it is.

> too far. An insurance company that, for example, slandered or assaulted an insured in the course of a claims dispute would not be immune from tort liability.

Choharis v. State Farm Fire & Casualty, 961 A.2d, at 1088.

Regarding Appellee's other points, which largely recite the district court's opinion in this case, and are otherwise re-workings of the contents of its initial motion to dismiss, Appellee disregards Appellants' ability to plead in the alternative. The district court went so far as to dismiss at least one of Appellants' claims (unjust enrichment) based upon Appellants having pled another theory of relief (breach of contract). *See* District Court Opinion (App 33, at 37-38). Rule 8 of the *Federal Rules of Civil Procedure* states that "[a] pleading that states a claim for relief must contain:…(3) a demand for the relief sought, which may include relief in the alternative or different types of relief." *Id.* A similar instance was analyzed by the United States District Court for the Southern District of New York, in a case in which one party argued that by pleading tortious interference with contract, the opposing party undermined its claim of interference with prospective economic advantage. *G-I Holdings, Inc. v. Baron & Budd*, 238 F. Supp. 2d 521, 534 (S.D.N.Y. 2002). While noting that these two (2) claims are conflicting, the district court in that case quoted FRCP 8, which states, in pertinent part:

> A party may set forth two or more statements of a claim or defense alternatively or hypothetically, either in one count or defense or in

> separate counts or defenses. When two or more statements are made in the alternative and one of them if made independently would be sufficient, **the pleading is not made insufficient by the insufficiency of one or more of the alternative statements. A party may also state as many separate claims or defenses as the party has regardless of consistency and whether based on legal, equitable, or maritime grounds**.

Id., at 535. (emphasis added).

The District Court for the Southern District of New York ultimately determined that, to preclude any of the party's claims on the basis of having pled other, potentially inapposite claims "would unfairly require [party] to choose, at an early stage in the proceedings, which cause of action to base its claim." *Id.*, at 536.

Appellants have made clear both in written and in oral arguments that, while it considers its contract with Appellee to be valid and enforceable, it does not rely whole-heartedly on that consideration which it knows not to be ironclad. In this instance, Appellants have set forth multiple theories of relief, and, like the case the Southern District of New York espoused upon, this case is still very much in its infancy. Appellants' claims should be reinstated, and discovery allowed to *begin* in this case.

CONCLUSION

The District Court of Appeals erred in this case in its blanket dismissal of nearly all of Appellants' claims, largely based upon a failure to plead actual damages, and the absence of a duty for Appellee to exercise due care in the

protection of its consumers' sensitive data. The lower court ignored clear factual allegations pleading actual damages. This Court, recently, in *OPM*, revived a similarly dismissed class action complaint in which it espoused its view that all of the plaintiffs pled actual damages sufficient to survive a 12(b)(6) motion to dismiss. In that case, many of the named plaintiffs' damages suffered were less than that of the class members here, who also alleged the theft of sensitive financial, in addition to biographical data. Finally, it is obvious that, due to increasing technological concerns, sensitive data which is required from consumes in order to purchase such necessary services such as health insurance, should come with a duty to safeguard it from those who profit directly from it and who are in a position to protect it. It is clear that the Appellants' claims were wrongfully dismissed, and the lower court's order should be reversed and remanded so that this case can truly begin in earnest.

Respectfully submitted,

/s/ *Christopher T. Nace*

Troy N. Giatras, Esq.
Bar Number: 429086
THE GIATRAS LAW FIRM, PLLC
118 Capitol St., Ste. 400
Charleston, WV 25301
Phone: 304.343.2900
troy@thewvlawfirm.com
Counsel for Appellants

Christopher T. Nace, Esq.
Bar Number 54503
PAULSON & NACE, PLLC
1025 Thomas Jefferson St. NW
Suite 810
Washington, D.C. 20007
Phone: 202.463.1999
ctnace@paulsonandnace.com
Counsel for Appellants

Jonathan B. Nace, Esq.
Bar Number 60148
NIDEL & NACE, PLLC
2201 Wisconsin Ave.NW
Suite 200
Washington, D.C. 20007
Phone: 202.780.5153
jon@nidellaw.com
Counsel for Appellants

RULE 32 CERTIFICATION

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because:

This brief contains 5,101 words in its entirety.

2. This brief complies with the typeface and type-style requirements of Federal Rules of Appellate Procedure 32(a)(5) and 32(a)(6) because:

This brief has been prepared in a proportionally spaced typeface using Microsoft Word 2019 in 14-point Time New Roman font.

/s/ *Christopher T. Nace*

CERTIFICATE OF SERVICE

I hereby certify that on this 14th day of August, 2019 a copy of the foregoing Reply Brief of Appellants was filed using the Court's ECF system as follows:

Matt Gatewood
Sutherland Asbill & Brennan LLP
700 Sixth Street, NW
Suite 700
Washington, D.C. 20001
Email Address: matthew.gatewood@sutherland.com
Counsel for Defendants-Appellees Carefirst, Inc., Carefirst of MD, CFBC, GHS

Robert D. Owen
Sutherland Asbill & Brennan LLP
The Grace Building, 40th Floor
1114 Avenue of the Americas
New York, NY 10036
Counsel for Defendants-Appellees Carefirst, Inc., Carefirst of MD, CFBC, GHS

This the 14th day of August, 2019.

/s/ *Christopher T. Nace*
Christopher T. Nace, Esq.

NOT YET SCHEDULED FOR ORAL ARGUMENT

No. 19-7020

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

CHANTAL ATTIAS, Individually and on behalf of all others similarly situated, *et al*.

Plaintiffs - Appellants,

v.

CAREFIRST, INC., *et al.*,

Defendants - Appellees.

On Appeal from the United States District Court for the District of Columbia, in Case No. 1:15-cv-882 (CRC), Christopher R. Cooper, Judge

ADDENDUM TO REPLY BRIEF OF APPELLANTS

Troy N. Giatras, Esq.
Bar Number: 429086
THE GIATRAS LAW FIRM, PLLC
118 Capitol St., Ste. 400
Charleston, WV 25301
Phone: 304.343.2900
troy@thewvlawfirm.com
Counsel for Appellants

Christopher T. Nace, Esq.
Bar Number 54503
PAULSON & NACE, PLLC
1025 Thomas Jefferson St. NW
Suite 810
Washington, D.C. 20007
Phone: 202.463.1999
ctnace@paulsonandnace.com
Counsel for Appellants

Jonathan B. Nace, Esq.
Bar Number 60148
NIDEL & NACE, PLLC
2201 Wisconsin Ave.NW
Suite 200
Washington, D.C. 20007
Phone: 202.780.5153
jon@nidellaw.com
Counsel for Appellants

TABLE OF CONTENTS

ADDENDUM: CONSOLIDATED AMENDED COMPLAINT.....A1

2016 WL 11218210 (D.D.C.) (Trial Pleading)
United States District Court, District of Columbia.

In Re: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION.

MDL-2664.

No. 15-1394 (ABJ).
March 14, 2016.

This Document Relates To: ALL CASES

Consolidated Amended Complaint

Daniel C. Girard, Jordan Elias, Esfand Y. Nafisi, Linh G. Vuong, Girard Gibbs LLP, 601 California Street, 14th Floor, San Francisco, CA 94108, (415) 981-4800, dcg@girardgibbs.com, Interim Lead Class Counsel.

David H. Thompson, Peter A. Patterson, Harold Reeves, Cooper & Kirk, PLLC, 1523 New Hampshire Avenue, N.W., Washington, D.C. 20036; Tina Wolfson, Theodore Maya, Bradley King, 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, Stueve Siegel Hanson LLP, 460 Nichols Road, Suite 200, Kansas City, MO 64112; Denis F. Sheils, Kohn, Swift & Graf, P.C., One South Broad Street, Suite 2100, Philadelphia, PA 19107; Graham B. LippSmith, Kasdan LippSmith Weber Turner LLP, 500 South Grand Avenue, Suite 1310, Los Angeles, CA 90071; Nicholas Koluncich III, The Law Offices of Nicholas Koluncich III, 500 Marquette Avenue N.W., Suite 1200, Albuquerque, NM 87102; Edward W. Ciolko, Kessler Topaz Meltzer & Check LLP, 280 King of Prussia Road, Radnor, PA 19087; Steven W. Teppler, Abbott Law Group, P.A., 2929 Plummer Cove Road, Jacksonville, FL 32223, Plaintiffs' Counsel.

I. NATURE OF THE ACTION

1. This action arises from the failure of Defendants the United States Office of Personnel Management ("OPM") and its security contractor KeyPoint Government Solutions, Inc. ("KeyPoint"), to establish legally required safeguards to ensure the security of government investigation information of current, former, and prospective employees of the federal government and its contractors. Defendants' failure to implement adequate, compulsory security measures in the face of known, ongoing, and persistent cyber threats—and despite repeated warnings of their systems' vulnerabilities—resulted in data breaches affecting more than 21 million people. The government investigation information ("GII") exposed and stolen in these breaches is private and sensitive, consisting of fingerprint records, detailed personal, financial, medical, and associational histories, Social Security numbers and birthdates of employees and their family members, and other private facts collected in federal background and security clearance investigations and stored on Defendants' electronic systems.

2. OPM announced a series of data breaches in 2015. For years before the announcement, OPM officials knew that OPM's systems lacked critical security safeguards and controls. Since 2007, audits carried out by the Office of Inspector General ("IG"), an independent office within OPM, warned that OPM's information security systems, management, and protocols were inordinately lax and vulnerable to electronic incursions. The OPM Inspector General's audits determined that OPM lacked not only the technology and oversight to protect its systems from cyberattacks but also the ability to discern the existence and extent of such an attack. OPM failed to remedy these known deficiencies and failed to follow its auditors' guidance for bringing its cybersecurity defenses into compliance with federal requirements.

3. OPM officials knew that OPM was a prime target for cyberattacks. OPM officials were aware of constant hacking attempts against OPM's systems. OPM's systems were breached in 2009 and 2012. A November 2013 attack compromised critical security documents.

4. Then in about December 2013, an unknown person or persons obtained the user log-in credentials of a KeyPoint employee. Those credentials were used to invade KeyPoint's systems and steal the personnel records of tens of thousands of Department of Homeland Security employees (the "KeyPoint Breach").

5. OPM learned in September 2014 of the December 2013 cyberattack on KeyPoint. OPM did not terminate or suspend its contract with KeyPoint, limit KeyPoint's access to OPM's systems, or take remedial actions necessary to protect OPM's systems from incursions made possible by the KeyPoint Breach.

6. Hackers used KeyPoint credentials to breach OPM's information systems in May 2014 and maintained access to OPM's information systems for over a year. Once inside OPM's network, the hackers gained access to another set of OPM servers stored in the Interior Department. The attacks begun in 2014 (the "OPM Breaches") went undetected for several months. By the time they were discovered, vast amounts of sensitive information had been extracted from OPM's network.

7. The victims of the KeyPoint Breach and the OPM Breaches (together, the "Data Breaches") have sustained economic harm from misuse of the stolen information, and their GII remains subject to a continuing risk of additional exposure or theft as a consequence of OPM's ongoing failure to secure it.

8. The IG issued its most recent audit of OPM's electronic systems in November 2015. The audit determined that most of the vulnerabilities exploited in the OPM Breaches still exist and, in some instances, have worsened. As in 2014, the IG advised OPM to shut down several of its major systems that are operating without security authorizations in violation of law. As in 2014, OPM has refused to do so, on the basis that accessibility of data to assist its continuing operations takes precedence over securing the confidentiality and integrity of the GII under its control.

9. Defendants' failure to protect GII, despite repeated official warnings of cyber threats and security lapses in their systems, constitutes willful misconduct. OPM, unlawfully prioritizing convenience over safety and ignoring direction from its federal auditors, violated the Privacy Act, the Federal Information Security Management Act, the Federal Information Security Modernization Act, and the Administrative Procedure Act and breached its contracts with Plaintiffs and Class members. KeyPoint's actions and inactions constitute negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and state statutes.

II. PARTIES

A. Plaintiffs

10. Plaintiffs bring this action on behalf of individuals whose sensitive personal information was compromised in the OPM Breaches or in the KeyPoint Breach. As used herein, "sensitive personal information" includes, at a minimum, Social Security numbers and birthdates, but may also include the range of GII compromised in the Data Breaches.

11. Plaintiff American Federation of Government Employees ("AFGE") is a labor organization headquartered at 80 F Street, N.W., Washington, D.C. 20001. AFGE represents, on its own and through its affiliated councils and locals, approximately 650,000 civilian employees in departments and agencies throughout the federal government, for a variety of purposes. AFGE conducts collective bargaining on behalf of employees it represents, and it works to ensure that its members' rights, including statutory and contractual rights, are honored and protected by their employers. Workers in virtually all domains of the federal government depend on AFGE for legal representation, legislative advocacy, technical expertise, and informational services.

12. In this action, AFGE seeks declaratory and injunctive relief only on behalf of the Class. OPM has notified hundreds of thousands of AFGE members that their GII was compromised in the OPM Breaches. AFGE has actively pursued and defended its members' rights and interests relating to this controversy, including by requesting that they be afforded

administrative leave to register for identity theft protection services and to manage any other fallout from the OPM Breaches, and by seeking lifetime identify theft protection services for all federal employees.

13. Plaintiff Travis Arnold resides and is domiciled in the state of Arizona. He formerly served in Field Artillery at the Department of Defense for approximately twelve years. Arnold provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, while reviewing his bank statement, Arnold discovered an unauthorized charge of approximately $125 for a purchase in China. He has spent approximately ten hours communicating with employees of his bank to reverse this fraudulent transaction and submitting documents detailing the fraud. While reviewing his credit report, Arnold also learned that between six and ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Arnold has spent many hours disputing these fraudulent inquiries. He suffers stress related to concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Arnold to review his credit reports and financial accounts with greater frequency.

14. Plaintiff Tony Bachtell resides and is domiciled in the state of Wisconsin. He currently works as a floor covering specialist at Orion Hardwood Floors, a federal government contractor. Bachtell provided sensitive personal information to the federal government. He and his wife received notice from OPM that such information has been compromised in the Data Breaches. In February 2016, the Internal Revenue Service informed Bachtell that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Bachtell has spent many hours attempting to resolve this tax fraud issue. Payment of his tax refunds will be delayed for several months. Also in February 2016, the Social Security Administration informed Bachtell that an unknown individual had used his and his wife's personal information to create online "My Social Security" accounts. Such accounts can be used to request a replacement Social Security card and to obtain estimates of a Social Security cardholder's future retirement benefits and the amount he or she has paid in Social Security and Medicare taxes. Thereafter, Bachtell learned that approximately ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Bachtell has devoted many hours to remedial actions, including placing a freeze on his credit and communicating with the Social Security Administration to terminate the unauthorized accounts. His exposure to the Data Breaches has also caused Bachtell to review his credit reports and financial accounts with greater frequency.

15. Plaintiff Ryan Bonner resides and is domiciled in the state of Pennsylvania. He formerly worked at the Transportation Security Administration, as a Transportation Security Officer. Bonner provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. His exposure to the Data Breaches has caused Bonner to review his credit reports and financial accounts with greater frequency.

16. Plaintiff Monty Bos resides and is domiciled in the state of Oklahoma. He currently works as a Processor with ASRC Federal Primus, a federal government contractor. Bos previously worked as a Tractor Operator for the Army's Directorate of Plans, Training, Mobilization, and Security. Bos provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Bos thereafter learned that an unauthorized credit card account had been opened in his name. He now reviews his credit reports every month to detect fraudulent activity.

17. Plaintiff Gardell Branch resides and is domiciled in the state of Illinois. He formerly worked as a Casual Mail Handler at the Postal Service. Branch provided sensitive personal information to the federal government, including in an SF-85 form, and received notice from OPM that such information has been compromised in the Data Breaches. Branch thereafter purchased monthly credit monitoring services from Equifax. Additionally, the Social Security Administration notified Branch that an unknown individual had attempted to use his Social Security Number. This incident required Branch to spend time verifying his identity and creating an identity theft profile with the Social Security Administration. His exposure to the Data Breaches has also caused Branch to review his financial accounts with greater frequency. He now reviews his bank and credit card accounts at least every other day to detect fraudulent activity.

18. Plaintiff Myrna Brown resides and is domiciled in the state of New Mexico. She formerly worked as an International Trade Specialist in the Foreign Commercial Service of the Commerce Department. Brown provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has

been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Brown to review her financial accounts with greater frequency. Brown now also reviews her credit reports regularly to detect fraudulent activity. Additionally, 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. Plaintiff Heather Burnett-Rick resides and is domiciled in the state of Michigan. She currently works as a Foreman with the Federal Bureau of Prisons, and formerly served in the National Guard for approximately twelve years. Additionally, Burnett-Rick applied to be a Border Patrol Agent with Customs and Border Protection and an Air Marshal with the Federal Air Marshal Service. She and her husband provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. CSIdentity Corporation ("CSID") thereafter informed Burnett-Rick that her work email address had been found on the "dark web." The dark web consists of parts of the World Wide Web that cannot be accessed with standard web technology or located with ordinary search engines or browsers and which use encryption to conceal the identity of those operating the websites. Dark websites are predominantly used to facilitate illicit activities, such as drug trafficking and identity theft. Burnett-Rick also learned from her bank that her debit card number had been used in an unauthorized attempt to make charges in Indiana of approximately $900, and that additional unauthorized charges of approximately $300 had been approved and deducted from her checking account. She spent about ten hours speaking with employees of her bank and reviewing and submitting affidavits and other documents to dispute these unauthorized charges. 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. Her exposure to the Data Breaches has also caused Burnett-Rick to review her financial accounts with greater frequency.

20. Plaintiff Robert Crawford resides and is domiciled in the state of Indiana. He currently works as an Operating Practices Inspector with the Federal Railroad Administration, and previously served in the Navy for approximately 29 years. Crawford provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Thereafter, Crawford placed fraud alerts on his credit and began reviewing his credit reports and financial statements every day.

21. Plaintiff Paul Daly resides and is domiciled in the state of Florida. He formerly worked as a Manager of Distribution Operations at the Postal Service, where he was employed for approximately 37 years. Daly's wife formerly worked at the Internal Revenue Service. Daly and his wife provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, the Internal Revenue Service informed Daly that fraudulent tax returns for the 2014 tax year had been filed using his and his wife's personal information (on separate tax return forms). Daly has spent many hours attempting to resolve these tax fraud issues, which remain under investigation by the Internal Revenue Service. Additionally, he closed financial accounts and opened new ones, and purchased credit monitoring services through Equifax, for which he pays $29.95 per month. His exposure to the Data Breaches has also caused Daly to review his financial accounts with greater frequency, and to refrain from online bill payment activities, which has caused him to incur $30.95 per month in fees to make payments over the phone for his wife's car and for their credit card and phone bills.

22. Plaintiff Jane Doe currently resides in Virginia and plans to relocate to Kentucky in May 2016 due to her husband's military transfer orders. She is using the pseudonym "Jane Doe" in this action because of her personal safety concerns. Doe currently works as an Information Technology Specialist Project Manager at the Department of Housing and Urban Development. She formerly worked at various federal agencies in positions that similarly involved monitoring and controlling computer systems. Doe's husband serves in the Army. Doe and her husband each provided sensitive personal information to the federal government, including in SF-86 forms. Doe and her husband each received notice from OPM that such information has been compromised in the Data Breaches. In August 2015, the Federal Bureau of Investigation informed Doe that her GII had been acquired by the so-called Islamic State of Iraq and al-Sham ("ISIS"). While reviewing her credit report, Doe discovered that twelve unknown accounts had been fraudulently opened in her name and were in collections. She paid approximately $198 to a credit repair law firm for assistance in closing the fraudulent accounts and removing them from her credit report. As of this filing, only some of these fraudulent accounts have been closed. When Doe attempted to access her credit report online with TransUnion, she found that she was unable to do so because TransUnion could not verify her identity. Doe has spent between 40 and 50 hours dealing with the fraudulent accounts, communicating with the FBI, and

attempting to gain access to her credit report with TransUnion. She expended approximately $50 to obtain copies of her credit report. Doe suffers stress resulting from concerns for her personal safety and that of her family members, and concerns that her exposure to the Data Breaches will impair her ability to obtain a job transfer and the Top Secret clearance needed to perform her job. Her exposure to the Data Breaches has also caused Doe to review her credit reports and financial accounts with greater frequency.

23. Plaintiff Jane Doe II resides and is domiciled in the state of Kansas. She is using the pseudonym "Jane Doe II" in this action because of her personal safety concerns. Doe II's spouse is an Assistant United States Attorney responsible for prosecuting large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families. Doe II's husband has received multiple death threats throughout his career and was the subject of an assassination attempt. Since that attempt, Doe II and her husband have used a P.O. Box miles from their home as their mailing address, and have maintained unlisted telephone numbers. Doe II and her husband have two minor children. Doe II's husband provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Doe II also received notice from OPM that her sensitive personal information has been compromised in the Data Breaches. Doe II experiences significant stress from fear that the exposure of her and her family members' sensitive personal information will cause them to be targeted for retaliatory attacks and bodily harm. Doe II also experiences stress from concerns that she and her family members face an increased risk of identity theft, fraud, and other types of monetary harm.

24. Plaintiff John Doe resides and is domiciled in the state of Washington. He is using the pseudonym "John Doe" in this action because of his personal safety concerns. He currently works as a Senior Inspector with the Marshals Service, where he has been employed for approximately 27 years. Doe holds a Top Secret clearance and has investigated drug trafficking cartels. Doe provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In February 2016, the Internal Revenue Service informed Doe that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Doe has spent five to ten hours attempting to resolve the tax fraud issue. Payment of his tax refunds is expected to be delayed for several months. Doe suffers stress resulting from concerns for his personal safety and that of his family members, and concerns that identity theft will aggravate his health problems and adversely affect his retirement plan.

25. Plaintiff John Doe II resides and is domiciled in the state of Idaho. He is using the pseudonym "John Doe II" in this action because of his personal safety concerns. He formerly worked for 20 years as a Senior Special Agent with the Customs Service, Office of Enforcement (which merged with Immigration and Naturalization Service, Investigations to form Immigration and Customs Enforcement, a division of the Department of Homeland Security, and was later renamed Homeland Security Investigations). As a member of the Joint Terrorist Task Force, Doe II supervised investigations of terrorism and drug trafficking cartels. His security clearance was above Top Secret, at the Sensitive Compartmented Information level. Doe II provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. He thereafter spent time to change his bank accounts, and he purchased credit monitoring services through LifeLock, for which he pays $329 annually. Doe II suffers stress resulting from concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Doe II to review his credit reports and financial accounts with greater frequency.

26. Plaintiff John Doe III resides and is domiciled in the state of Virginia. He is using the pseudonym "John Doe III" in this action because of his personal safety concerns. Doe III is an independent contractor who works with a federal government contractor. He previously served in the Army. Doe III provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. The Internal Revenue Service thereafter informed Doe III that a fraudulent tax return had been filed using his personal information. Doe III has spent several hours attempting to resolve this tax fraud issue. Payment of his tax refunds will be delayed. His exposure to the Data Breaches has also caused Doe III to review his financial accounts with greater frequency. He now spends approximately one hour per day reviewing his financial accounts to detect fraudulent activity.

27. Plaintiff Michael Ebert resides and is domiciled in the state of Nevada. Ebert worked for the federal government and its contractors for approximately 45 years. He served for 20 years in the Army. Ebert provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Ebert's wife also received notice from OPM that her sensitive personal information has

been compromised in the Data Breaches. His exposure to the Data Breaches has caused Ebert to review his financial accounts with greater frequency. He now reviews his bank and credit card accounts approximately twice per day to detect fraudulent activity.

28. Plaintiff Kelly Flynn resides and is domiciled in the state of Utah. She currently works as a Staff Assistant at the Interior Department's Office of the Solicitor. She formerly worked at the Air Force, the Navy, the Internal Revenue Service, and the Postal Service. Flynn provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In spring 2015, the Internal Revenue Service informed Flynn that a fraudulent tax return for the 2014 tax year had been filed using her and her husband's personal information. The investigation into this tax fraud issue remains pending. As a result, Flynn has not yet received her federal or state income tax refunds for the 2014 tax year. In July 2015, after learning of the Data Breaches, Flynn added credit monitoring from the three major credit bureaus, at a cost of $10 per month, to her preexisting credit and identity monitoring services. Flynn thereafter learned that a Barclays Bank credit card and a JCPenney credit card had been fraudulently opened in her name. Flynn's husband also learned that two credit card accounts had been fraudulently opened in his name. Additionally, Equifax notified Flynn that a $5,000 loan from Cash Central had been taken out in her name online, and that the loan was delinquent and in collections. On March 1, 2016, Flynn's husband learned that a loan of over $1,400 with Castle Creek Payday Loans had been taken out in his name online, and was delinquent. Flynn has spent over 50 hours attempting to resolve the tax fraud issues and to close the fraudulent accounts and terminate the fraudulent loans. Her exposure to the Data Breaches has also caused Flynn to review her credit reports and financial accounts with greater frequency. Flynn suffers stress resulting from concerns that her and her family members' identities will be stolen.

29. Plaintiff Alia Fuli resides and is domiciled in the state of Nevada. She currently works as a Service Representative at the Social Security Administration, and formerly worked as a Medical Reimbursement Technician and Patient Accounts Representative at the Department of Veterans Affairs. Fuli began working for the Department of Veterans Affairs in 2011. Fuli provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2015, Fuli learned that a PayPal/Synchrony Bank credit card account had been opened in her name and used to make unauthorized online purchases of approximately $298. Fuli has spent approximately 15 hours communicating with PayPal representatives in an attempt to get these charges reversed and the fraudulent account closed. While reviewing her credit report, Fuli also learned that between July 2015 and December 2015, multiple inquiries regarding her credit had been made by companies with which she had no prior relationship. Her exposure to the Data Breaches has caused Fuli to review her credit reports and financial accounts with greater frequency.

30. Plaintiff Johnny Gonzalez resides and is domiciled in the state of Florida. He currently works as a Deportation Officer at Immigrations and Customs Enforcement, and formerly worked as a Border Patrol Agent at Customs and Border Protection. Gonzalez provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Gonzalez's bank thereafter informed him that his debit card number had been used to make unauthorized charges of approximately $360 in China. In January 2016, Gonzalez's bank informed him that an unauthorized attempt had been made to charge approximately $1,000 on his debit card number in Florida, and that an additional $96 in unauthorized charges had been approved and deducted from his checking account. In late 2015, Gonzalez also learned that his credit card number had been used to make an unauthorized charge of approximately $100 in Massachusetts. Gonzalez has spent approximately 20 hours attempting to reverse the fraudulent financial transactions and closing his checking account with his bank and opening a new account. 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. His exposure to the Data Breaches has also caused Gonzalez to review his financial accounts with greater frequency.

31. Plaintiff Lillian Gonzalez-Colon resides and is domiciled in the state of Florida. She currently works as a Medical Technologist at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2012. Gonzalez-Colon provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2014, Gonzalez-Colon learned that a series of inquiries regarding her credit had been made in connection with an unauthorized attempt to open fraudulent accounts in her name. In January 2015, the Internal Revenue Service informed Gonzalez-Colon that an unknown individual had fraudulently claimed her 4-year-old son as a dependent on a tax return filed in New York for the 2014 tax year. As a result, payment of her tax refunds was delayed for three months. In February 2016, Gonzalez-Colon's mortgage lenders informed her that an

account with Verizon Wireless had been opened in her name in December 2014 and that this account had an outstanding balance of almost $3,000. The fraudulent account remains under investigation by Verizon Wireless. Gonzalez-Colon has spent over 100 hours in attempts to resolve the fraudulent tax return filing and to close the fraudulent Verizon Wireless account. These efforts required her to take time off work. Her exposure to the Data Breaches has caused Gonzalez-Colon to review her credit reports and financial accounts with greater frequency. Gonzalez-Colon suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future.

32. Plaintiff Orin Griffith resides and is domiciled in the state of Oklahoma. Griffith currently serves as an Aircraft Mechanic in the Air Force, and formerly served as an Aircraft Weapons Mechanic in the Army. Griffith provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In February 2015, the Internal Revenue Service informed Griffith that a fraudulent tax return for the 2014 tax year had been filed using his and his wife's personal information. Griffith has spent several hours attempting to resolve this tax fraud issue. Payment of his tax refunds was delayed for almost ten months. Griffith's exposure to the Data Breaches has caused him to review his financial accounts with greater frequency.

33. Plaintiff Jennifer Gum resides and is domiciled in the state of Kansas. She works as a Medical Reimbursement Technician for the Veterans Affairs Medical Center, and her husband works as a Senior Corrections Officer with the Federal Bureau of Prisons. She began working for the Department of Veterans Affairs in 2011. Gum and her husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Gum to review her financial accounts with greater frequency.

34. Plaintiff Michael Hanagan resides and is domiciled in the state of California. He currently works as a Capital Habeas Staff Attorney in the United States District Court for the Central District of California. Hanagan provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Hanagan thereafter purchased a monthly subscription for credit and identity monitoring and purchased copies of his credit reports to detect fraudulent activity.

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

36. Plaintiff Deborah Hoffman resides and is domiciled in the state of Texas. She currently works as a transcriptionist with Datagain, a federal government contractor. Hoffman provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Hoffman to review her financial accounts with greater frequency. She now checks her bank and credit card accounts daily to detect fraudulent activity.

37. Plaintiff Michael Johnson resides and is domiciled in the state of Washington. He currently works as a project director for Camo2Commerce, a federal government contractor. Johnson previously worked in military and federal government positions for over 30 years. He was Chief of Operations for the Multi-National Force in Iraq, a Military Police Officer in the Air Force, and a Platoon Leader in the Army. Johnson also worked as an investigator for KeyPoint. Johnson provided sensitive personal information to the federal government, including in an SF-86 form. He and his wife separately received notice from OPM that such information has been compromised in the Data Breaches. As a retired Senior Army Officer and former Chief of Operations in Iraq, Johnson experiences significant stress from fear that the exposure of his and his family's sensitive personal information will cause him and his family to be targeted for retaliatory attacks and bodily harm. His exposure to the Data Breaches has also caused him to review his financial accounts with greater frequency.

38. Plaintiff Cynthia King-Myers resides and is domiciled in the state of Illinois. She is currently employed as a Social Worker at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2013. King-Myers provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, King-Myers learned that unauthorized charges of

approximately $658 had been incurred on her debit card account. King-Myers has spent between 30 and 35 hours attempting to reverse these fraudulent transactions. Her exposure to the Data Breaches has also caused King-Myers to review her credit reports and financial accounts with greater frequency.

39. Plaintiff Ryan Lozar resides and is domiciled in the state of New York. He formerly worked as a Law Clerk in the United States District Court for the Eastern District of New York, a Law Clerk in the United States District Court for the District of Puerto Rico, and a Special Assistant United States Attorney in the United States Attorney's Office for the Southern District of California. Lozar provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Lozar thereafter learned that an unknown individual had opened a PayPal account in his name and received a $1,000 cash advance. He also learned that an unknown individual had opened a Best Buy account in his name and used it to purchase $3,500 worth of merchandise. Lozar spent many hours communicating with PayPal and Best Buy to dispute and resolve these fraudulent activities. Lozar then placed a freeze on his credit and contacted the three major credit bureaus to confirm that they were aware of the fraud. Lozar thereafter paid $15 to lift the credit freeze to allow a legitimate inquiry on his credit to be made.

40. Plaintiff Teresa J. McGarry resides and is domiciled in the state of Florida. She currently works in the Social Security Administration as an Administrative Law Judge. McGarry previously served as an Assistant United States Attorney and as a Judge Advocate General with the Navy. McGarry provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. McGarry thereafter purchased a monthly subscription for credit and identity monitoring. Her exposure to the Data Breaches has also caused McGarry to review her financial accounts with greater frequency.

41. Plaintiff Charlene Oliver resides and is domiciled in the state of Mississippi. She formerly served in the Navy, as a Torpedoman's Mate. Oliver's husband formerly served in the Army, as a Captain of Artillery. Oliver and her husband provided their sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In June 2015, Oliver received a letter from her electricity utility company informing her that her account had been closed, was no longer in her name, and had incurred charges of $500. Oliver also learned that an unknown individual had accessed her electricity account online using her Social Security number and maiden name. Thereafter, her electricity utility company sent her a deposit check for the closed account, but in someone else's name. Oliver has devoted many hours to communicating with her electricity utility company to reverse the fraudulent charges and reopen an account in her name. Her dispute with the company, which claims she must pay another security deposit of $390, is unresolved. Additionally, Oliver learned that fraudulent purchases had been made using her debit card and two credit card numbers. Oliver has spent several hours communicating with her bank and credit card companies to reverse these fraudulent transactions, and she purchased credit monitoring and repair services through a credit repair law firm, for which she pays $100 per month. Her exposure to the Data Breaches has also caused Oliver to review her financial accounts with greater frequency.

42. Plaintiff Toralf Peters resides and is domiciled in the state of Alabama. He is currently a partner of Telesto Group, a subcontractor for the Interior Department and a former subcontractor for the Department of Defense. Peters provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Among other things, Peters's exposure to the Data Breaches has caused him to review his credit reports and financial accounts with greater frequency. Peters also suffers stress resulting from concerns that his fingerprints and sensitive personal information will be used to attempt to steal his identity.

43. Plaintiff Mario Sampedro resides and is domiciled in the state of California. He currently works as a Special Agent at the Department of Homeland Security, a position he has held for 26 years. Sampedro provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Sampedro suffers stress resulting from concerns for his personal safety and that of his family members, and concerns regarding the unauthorized use of their sensitive personal information. Sampedro, who is nearing retirement from Homeland Security, worries that the theft of his sensitive personal information will impair his ability to secure future employment with government contractors. His exposure to the Data Breaches has caused Sampedro to review his financial accounts with greater frequency.

44. Plaintiff Timothy Sebert resides and is domiciled in the state of Georgia. Sebert currently works as a Language Analyst

for the Navy, where he has served for more than eight years. Sebert and his wife provided sensitive personal information to the federal government, including in SF-86 forms, and received notice from OPM that such information has been compromised in the Data Breaches. Sebert suffers stress resulting from concerns for his personal safety and that of his family members and concerns regarding the unauthorized use of their sensitive personal information. Sebert spent more than five hours reviewing the information in his electronic tax filing account multiple times and changing his account credentials to decrease the chances of his tax refunds being stolen. His exposure to the Data Breaches has also caused Sebert to review his financial accounts with greater frequency.

45. Plaintiff Zachary Sharper resides and is domiciled in the state of Virginia. He currently works as a Contract Specialist Supervisor with the Department of Defense, Defense Logistics Agency. Sharper previously worked as a Corrections Officer at the Bureau of Prisons and a Fuel Systems Operator for the federal government contractor Kellogg Brown & Root. Additionally, Sharper served in the Army for approximately seven years. He provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Sharper thereafter learned accounts had been opened in his name with Sprint and Verizon Wireless, and that six iPhones had been ordered using those accounts. Sharper also received prepaid Green Dot cards he had not ordered. He has spent many hours attempting to resolve these fraudulent transactions.

46. Plaintiff Robert Slater resides and is domiciled in the state of Washington. He currently serves as a Signal Officer, and previously served as a Patriot Missile Operator, in the Army. Slater provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Slater suffers stress resulting from concerns that the theft of his sensitive personal information will impair his ability to obtain a higher security clearance, or future employment with a government contractor when he leaves the Army. His exposure to the Data Breaches has also caused Slater to review his financial accounts and credit reports with greater frequency to detect fraudulent activity.

47. Plaintiff Darren Strickland resides and is domiciled in the state of North Carolina. Strickland worked for many years for federal government contractors. Strickland provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. His exposure to the Data Breaches has caused Strickland to review his financial accounts with greater frequency.

48. Plaintiff Peter Uliano resides and is domiciled in the state of New Hampshire. He applied for and was offered a position as a Security Screener with the Transportation Security Administration. Uliano provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Among other things, his exposure to the Data Breaches has caused Uliano to review his financial accounts with greater frequency.

49. Plaintiff Nancy Wheatley resides and is domiciled in the state of Tennessee. She currently works as a registered nurse at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2011, and formerly served in the Army and in the National Guard. Wheatley provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. She thereafter learned that unknown individuals had opened fraudulent accounts in her name with Sprint and Virgin Mobile and that unauthorized online purchases had been made using her debit card number. Wheatley has spent many hours attempting to close the fraudulent accounts and to reverse the fraudulent transactions. Her exposure to the Data Breaches has also caused Wheatley to review her financial accounts with greater frequency.

50. Plaintiff Kimberly Winsor resides and is domiciled in the state of Kansas. She is currently employed as a Social Worker at the Department of Veterans Affairs in Kansas City. She began working for the Department of Veterans Affairs in 2015. Winsor and her husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, Winsor's husband learned from their bank that his debit card number had been used to make unauthorized purchases in Mississippi. On July 23, 2015, Winsor learned from their bank that her debit card number had been used to make unauthorized purchases in Texas. On November 24, 2015, CSID informed Winsor that her 8-year-old son's Social Security number had been used in California for an unknown purpose. Winsor has spent approximately twelve hours attempting to resolve the fraudulent transactions and the misuse of her son's Social Security number. Among other things, she made trips to her bank to obtain sensitive identifying documents, and

completed and submitted affidavits to dispute the fraudulent purchases. Winsor suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future. Her exposure to the Data Breaches has also caused Winsor to review her financial accounts with greater frequency.

B. Defendants

51. Defendant the United States acted through the Office of Personnel Management.

52. Defendant OPM is a federal agency headquartered at 1900 E Street, N.W., Washington, D.C. 20415. OPM handles many parts of the federal employee recruitment process and, in doing so, collects and maintains federal job applicants' GII, including information provided in background check and security clearance forms. OPM oversees more than two million background checks annually, provides human resources services to other agencies, and audits agency personnel practices.

53. Defendant KeyPoint is a private investigation and security firm incorporated in Delaware. KeyPoint is headquartered and maintains its principal place of business in Loveland, Colorado. KeyPoint provides fieldwork services for federal background and security clearance checks and employs or contracts with individuals in every state who assist with such investigations.

III. JURISDICTION AND VENUE

54. This Court has subject matter jurisdiction over all the federal claims in this action pursuant to 28 U.S.C. § 1331. The Court also has subject matter jurisdiction over the Privacy Act claim pursuant to 5 U.S.C. § 552a(g)(1)(D) and over the Little Tucker Act claim pursuant to 28 U.S.C. § 1346(a).

55. This Court has subject matter jurisdiction over the claims in this action against KeyPoint pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different from KeyPoint's state of citizenship, the total amount in controversy exceeds $5 million, and the proposed Class contains more than 100 members.

56. This Court has personal jurisdiction over OPM because it is headquartered in the District of Columbia and much of the relevant conduct occurred here.

57. This Court has personal jurisdiction over KeyPoint because it conducts significant business in the District of Columbia and much of the relevant conduct occurred here.

58. Venue is proper in this District under 28 U.S.C. § 1391 because OPM is located in the District of Columbia and a substantial part of the events and omissions giving rise to these claims occurred here.

59. Venue is also proper in this District under 5 U.S.C. §§ 552a(g)(5) and 703.

IV. COMMON ALLEGATIONS OF FACT

A. OPM and KeyPoint Collect and Store Confidential Information About Millions of Federal Job Applicants

60. OPM manages the recruitment and retention of the work force of the United States government. As part of its duties, OPM conducts background checks of prospective employees and security clearance checks of current and prospective employees. More than 100 federal agencies depend on OPM's investigatory products and services. OPM oversees more than two million investigations per year, at least 650,000 of which are to support security clearance determinations.

61. As part of its investigatory mandate, OPM collects and stores an enormous amount of information about federal job

applicants and past and present federal employees.

62. OPM's Federal Investigative Services division oversees the agency's background and security clearance checks.

63. Federal Investigative Services relies on a software system known as "EPIC." EPIC aggregates and stores information about federal job applicants, including information provided in electronic questionnaires and used in background and security clearance checks. Some of the data in EPIC is sufficiently sensitive that it is housed at the National Security Agency.

64. Among the data stored in EPIC are the master records from investigations of government employees.

65. EPIC also stores the Central Verification System, which contains most background and security clearance check information.

66. The Central Verification System stores versions of Standard Form 86 ("SF-86") as completed by federal job applicants and employees. SF-86 is a 127-page form that every federal job applicant and employee being considered for a security clearance must fill out and submit.

67. SF-86 contains, among other information, applicants' psychological and emotional health history, police records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants.

68. Each SF-86 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-86 form also states that the information provided in it "may be disclosed without your consent … as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-86 lists eleven permitted uses.

69. Applicants for non-sensitive federal government or contractor positions must fill out and submit an SF-85 form. Each SF-85 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-85 form also states that the information provided in it "may be disclosed without your consent … as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85 lists eleven permitted uses.

70. Applicants for "public trust" federal government or contractor positions must fill out and submit an SF-85P form. Each SF-85P form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-85P form also states that the information provided in it "may be disclosed without your consent … as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85P lists eleven permitted uses.

71. The Central Verification System stores completed versions of forms SF-85 and SF-85P.

72. The Central Verification System also contains polygraph data, fitness determinations, and decisions made pursuant to Homeland Security Presidential Directive (the background check determinations required for government employees and contractors to gain access to federal facilities).

73. Additionally, the Central Verification System contains detailed information relating to Personal Identification Verification ("PIV") Cards, which are government ID smart cards that government employees and contractors use to access government facilities and software systems.

74. The Electronic Official Personnel Folder is another OPM system that stores personnel files on individual federal employees. The information in such files includes birth certificates, job performance reports, resumes, school transcripts, military service records, employment history and benefits, and job applications that contain Social Security numbers and birthdates.

75. OPM hires contractors to carry out the investigative fieldwork necessary for background and security clearance investigations. KeyPoint performs the majority of OPM's fieldwork. As a contractor of OPM, KeyPoint is subject to the

requirements of the Privacy Act to the same extent as OPM. As of June 2015, KeyPoint had received more than $605 million under its OPM contract, with a funding cap of approximately $2.5 billion.

76. To perform its fieldwork, KeyPoint relies on systems that are electronically connected to those of OPM. This linkage allows KeyPoint employees and contractors to download from OPM's network information needed to conduct an investigation, and to upload investigatory findings to OPM's network. The system through which KeyPoint transmits data to and from OPM's network is called the Secure Portal. The Secure Portal is an electronic conduit through which, among other things, KeyPoint investigators access completed forms and other information stored in OPM's Central Verification System.

77. KeyPoint disseminates its Privacy Policy on the Internet. The policy states that KeyPoint is a consumer reporting agency. The policy further states that KeyPoint is required by the Fair Credit Reporting Act, 15 U.S.C. § 168, *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.

B. OPM's Prior Data Breaches and Failures to Comply with Federal Cybersecurity Standards and Audit Directions

78. At least two cyberattacks against OPM were publicly disclosed in the years leading up to the Data Breaches. In 2009, OPM's website and database for USAJOBS.gov—the employment website used by the federal government—was hacked by unknown persons who gained access to millions of users' private information. In May 2012, an unknown person or group infiltrated an OPM database, stole OPM user credentials (including user IDs and passwords), and posted those credentials online.

79. In addition to these cyberattacks, OPM was and is aware that its network is the subject of at least 10 million unauthorized electronic intrusion attempts every month.

80. At all relevant times, OPM also was aware of several successful cyberattacks against other federal agencies and government institutions. OPM was aware of at least the following data breach incidents: a May 2012 hack into the Bureau of Justice Statistics of the Department of Justice, a May 2012 hack of the Thrift Savings Plan, a June 2012 hack of the Commodity Futures Trading Commission network, a June 2012 incursion into a Department of Homeland Security website, and a September 2012 breach of personnel data maintained by the Navy.

i. The Inspector General's Annual FISMA Audits of OPM

81. From 2002 to 2014, the Federal Information Security Management Act governed software system requirements for federal agencies and contractors. 44 U.S.C. § 3541, *et seq.* The President signed the Federal Information Security Modernization Act of 2014 into law on December 18, 2014. That statute updates and supersedes the Federal Information Security Management Act. As used in this Complaint, "FISMA" means either the Federal Information Security Management Act of 2002 or the Federal Information Security Modernization Act of 2014, or both.

82. FISMA requires OPM to develop and implement policies, procedures, and guidelines on information security, and to comply with federal information security standards that FISMA makes compulsory and binding on OPM.

83. Agencies subject to FISMA must develop, implement, and maintain a security program that assesses information security risks and provides adequate security for the operations and assets of programs and software systems under agency and contractor control.

84. The IG, an independent office within OPM, conducts annual audits of OPM's cybersecurity program and practices in accordance with FISMA reporting requirements established by the Department of Homeland Security.

85. The purpose of the IG's audit function is to evaluate and ensure OPM's compliance with the information security

requirements of FISMA. Pursuant to FISMA, the IG is required to review several facets of OPM's information security program.

86. In each annual audit from 2011 to 2014, the IG found that OPM maintained an adequate capital planning and investment program for funding information security. In each of those years, however, the IG found that OPM had not fulfilled its information security obligations under federal law.

87. In the reporting of audit results, non-negligible security concerns of the IG are termed "significant deficiencies." More serious concerns that the IG determines pose an immediate risk to the security of assets or operations are termed "material weaknesses."

88. In each annual audit from 2007 to the present, the IG found that OPM's information security policies and practices suffered from material weaknesses.

89. Due to these material weaknesses and other information security deficiencies, OPM failed to comply with FISMA from 2007 to the present.

ii. Material Weaknesses Relating to Information Security Governance

90. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols were not in compliance with FISMA. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols contained material weaknesses that posed a significant threat to its systems. OPM failed to materially correct the deficiencies reported by the IG in these areas.

91. From 2007 to 2009, the IG found that OPM lacked required policies and procedures for managing information security. In 2009, the IG also found that, to the extent information security policies and procedures did exist at OPM, they had not been tailored to OPM with appropriate procedures and implementing guidance.

92. In 2009, the IG expanded the material weakness rating to cover OPM's overall information security governance program and information security management structure. A Flash Audit Alert from the IG in May 2009 identified four primary deficiencies:

a. OPM misrepresented the status of its information security program;

b. OPM's security policies and procedures were severely outdated;

c. OPM's security program was understaffed; and

d. OPM had been operating for over 14 months without a senior information security official.

93. In the 2010 FISMA audit, the IG again found that OPM's information security governance constituted a material weakness. In the 2010 FISMA audit, the IG faulted OPM for failing to remedy or otherwise address most of the deficiencies found in the 2007, 2008, and 2009 audits. OPM's policies, according to the IG, failed to provide employees with adequate guidance to secure OPM's information systems. In response, OPM stated its intent to implement comprehensive information security and privacy changes in fiscal year 2011.

94. In the 2011 FISMA audit, the IG found that OPM still lacked necessary security policies and procedures, including for agency-wide risk management, monitoring of security controls, and oversight of systems operated by a contractor. OPM's security policies again were not tailored to OPM's systems and were unaccompanied by needed guidance. The IG determined that OPM lacked a centralized security structure. Officials at various OPM divisions were responsible for testing and maintaining their own information security measures, without the guidance or oversight of the Chief Information Officer. The IG advised OPM to centralize its management structure to ensure coordinated implementation of needed information security upgrades. The IG also found that many of OPM's information security officers were not actually information security

professionals. These officers had been tasked with security functions in addition to their other full-time roles at OPM. The IG reported that OPM still was not providing appropriate guidance to its employees concerning management of systems risks.

95. By 2012, OPM had begun hiring information security professionals and centralizing its information security management structure. Nevertheless, the IG maintained its material weakness rating in its 2012 audit. In that audit the IG stated that OPM had only hired enough information security professionals to manage about one-third of OPM's information systems and that the new professionals had not performed any tangible work.

96. OPM contested the 2012 material weakness rating on the grounds that it had not suffered any loss of financial or personal information. The IG rejected OPM's position, stating that OPM's systems had, in fact, been breached on numerous occasions, resulting in the loss of sensitive data.

97. In 2013, the IG reiterated its material weakness rating of OPM's information security governance. The IG also noted that, since its last audit, OPM had not hired more security officers, thereby failing to remedy or otherwise address a central IG concern from previous years.

98. The IG's 2014 audit found that OPM still lacked a centralized cybersecurity team of individuals responsible for overseeing all of OPM's cybersecurity efforts and that OPM remained non-compliant with many FISMA requirements. The IG upgraded OPM's information security governance program from a "material weakness" to a "significant deficiency" rating, based on imminently planned improvements. The IG warned that it would reinstate the material weakness rating as to information security governance if the proposed changes were not made.

iii. Material Weaknesses Relating to Security Assessments and Authorizations of OPM Systems

99. FISMA requires OPM to certify that its information systems' technological security controls meet applicable requirements and to decide whether to authorize operation of an information system and accept the associated risk. FISMA's requirement that OPM certify and accredit system security controls is known as Security Assessment and Authorization.

100. The IG's 2010 FISMA audit found that OPM's process for certifying and accrediting system security controls was incomplete, inconsistent, of poor quality, and characterized by material weaknesses. The deficiencies stemmed in part from the fact that OPM's security officers lacked information security experience and training and were not subject to a centralized security management structure. Six OPM systems had expired authorizations in 2010, and another system had been in use for several years without being validly authorized.

101. In 2014, the IG reinstated the material weakness rating after having removed OPM's process for certifying and accrediting system security controls as a security concern in 2012 and 2013. Of the 21 OPM systems due to be authorized in 2014, eleven authorizations had not been completed. The IG recommended that OPM levy administrative sanctions on several OPM divisions, including Federal Investigative Services, whose systems were operating without valid authorizations.

102. The OPM systems operating without authorizations in 2014 included some of OPM's most critical and sensitive applications. One was a general system that supported and provided the electronic platform for approximately two-thirds of all information systems operated by OPM. Two other OPM systems operating without authorizations in 2014 were used by OPM's Federal Investigative Services division. Weaknesses in the information systems of this division, the IG warned OPM, raised national security implications.

103. The IG determined in 2014 that the lack of valid authorizations of OPM's systems was a critical and time-sensitive problem. The IG found OPM had failed to ensure that the security controls for its systems were working. The IG also found OPM lacked a way to monitor these systems for cyberattacks or data breaches. Based on these findings, the IG advised OPM to shut down all systems lacking a current and valid authorization. The IG's advice was unprecedented.

104. OPM chose not to follow the IG's 2014 recommendation to shut down the unauthorized systems.

iv. Other Deficiencies in OPM's Security Controls

105. OPM officials were aware of several other information security deficiencies summarized below. The deficiencies summarized below existed within OPM's systems immediately prior to the OPM Breaches. Each was identified and described in IG audits.

106. OPM failed to implement or enforce multi-factor authentication. OPM's failure to implement or enforce multi-factor identification increased the risk of a breach of OPM's information systems. Multi-factor authentication improves data security because a user needs more than one form of credential to access software systems. For example, the user inputs a password and also scans a PIV card with an embedded microchip. In 2011, Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 became binding on OPM. Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 require OPM to implement multi-factor authentication with PIV for its information systems. Immediately prior to the OPM Breaches, none of OPM's major information systems required PIV authentication.

107. OPM failed to promptly patch or install security updates for its systems. OPM's failure to patch or install security updates increased the vulnerability of OPM's systems to breach.

108. OPM lacked a mature vulnerability scanning program to find and track the status of security weaknesses in its systems. OPM lacked a centralized network security operations center to continuously monitor security events, and failed to continuously monitor the security controls of its software systems.

109. When employees accessed OPM's systems from a remote location, the remote access sessions did not terminate or lock out as required by FISMA. As a result, connections to OPM's systems were left open and vulnerable.

110. OPM lacked the ability to detect unauthorized devices connected to its network.

111. OPM failed to engage in appropriate oversight of its contractor-operated systems.

112. OPM failed to comply with several standards to which FISMA requires it to adhere, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, and contingency planning. 40 U.S.C. § 11331.

113. Only 37 of OPM's 47 software systems had been adequately tested for security in 2014, and it had been over eight years since all systems were tested.

C. Cyber Attackers Breach the Systems of OPM's Contractors

114. In or around December 2013, cyber attackers breached the information systems of KeyPoint and U.S. Investigations Services ("USIS") without being detected. At the time, KeyPoint and USIS were the primary contractors responsible for conducting the fieldwork for OPM's background and security clearance investigations.

115. In June 2014, USIS detected a breach of its systems and informed OPM that thousands of government employees' personal information might have been compromised. USIS ultimately sent out 31,000 notices of this data breach to federal employees.

116. Following the USIS breach, OPM rescinded its contracts with USIS. At the time, USIS was performing approximately 21,000 background checks per month. KeyPoint doubled the size of its work force to staff its additional responsibilities. KeyPoint failed to concurrently increase managerial oversight given its increased staff and additional responsibilities.

117. The December 2013 KeyPoint Breach was detected in September 2014. The nature and scope of the KeyPoint Breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

118. Following the disclosure of the KeyPoint Breach, the United States Customs Service and Border Protection suspended

all investigations being conducted on its behalf by KeyPoint until KeyPoint took steps to protect GII in and connected to KeyPoint's systems.

119. OPM did not suspend KeyPoint's investigations, rescind its contract with KeyPoint, prevent or limit KeyPoint's access to OPM systems, or take any measure adequate to mitigate the potential adverse effects of the KeyPoint Breach.

120. On April 27, 2015, OPM alerted more than 48,000 federal employees that their personal information might have been exposed in the KeyPoint Breach.

121. KeyPoint lacked software logs to track malware entering its systems and data exiting its systems. Precisely how the KeyPoint Breach occurred has not been disclosed.

122. By unreasonably failing to safeguard its security credentials and Plaintiffs' and Class members' GII, KeyPoint departed from its mandate, exceeded its authority, and breached its contract with OPM.

123. The contract between OPM and KeyPoint incorporates the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1). KeyPoint violated the Privacy Act and breached its contract with OPM 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, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members. KeyPoint also violated the Privacy Act and breached its contract with OPM by disclosing Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose.

124. In addition to departing from the commands and directives of federal law, KeyPoint acted negligently in performing its obligations under its contract with OPM.

D. Cyber Attackers Breach OPM's Systems

i. The Information Technology Documents Breach (November 2013)

125. On November 1, 2013, OPM's network was infiltrated. No GII was stolen. The hackers stole security system documents and electronic manuals concerning OPM's information technology assets. The stolen information provided a blueprint to OPM's network.

126. When OPM later announced this breach to the public, OPM disclosed only that no GII had been compromised; it did not disclose the theft of its security system documents and information technology manuals.

ii. The Background Investigation Breach (May 2014)

127. On May 7, 2014, hackers accessed OPM's network using stolen KeyPoint credentials. Once inside OPM's network, they installed malware and created a conduit through which data could be exfiltrated.

128. The nature and scope of the May 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive information for improper use.

129. The May 2014 breach was not detected for almost a year. It resulted in the theft of nearly 21.5 million background investigation records, including many million questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information of Class members.

130. The two primary systems the hackers targeted, and from which they removed data, were (i) the Electronic Official Personnel Folder system, and (ii) the database associated with the EPIC software used by the Federal Investigative Services office to collect information for government employee and contractor background checks.

iii. The Personnel Records Breach (October 2014)

131. No later than October 2014, hackers launched another successful cyberattack against OPM systems maintained in an Interior Department shared-services data center. The October 2014 breach resulted in the loss of approximately 4.2 million federal employees' personnel files.

132. The nature and scope of the October 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

133. Because OPM's systems were not shielded through multi-factor authentication or privileged access controls, the hackers were able to use the stolen KeyPoint credentials to access systems within OPM's network at will. During the several months in which the intruders maintained such access, they removed millions of personnel records via the Internet, hidden among normal traffic.

E. Causes of the OPM Breaches

134. Millions of unauthorized attempts to access sensitive United States government data systems take place each month. OPM's prioritization of accessibility and convenience over security foreseeably heightened the risk of a successful intrusion into OPM's systems. OPM's decisions not to comply with FISMA requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year without being detected.

135. OPM's inadequate patching of software systems contributed to the OPM Breaches. When a security flaw in a software system is discovered, the developer of that system often will create and recommend installing an update—or "patch"—to eliminate that vulnerability. Failure to promptly install such a patch exposes a software system to known and preventable risks. 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.

136. Other known deficiencies that contributed to the OPM Breaches include OPM's failures to establish a centralized management structure for information security, to encrypt data at rest and in transit, and to investigate outbound network traffic that did not conform to the Domain Name System ("DNS") Protocol.

137. Additionally, OPM's sub-networks were not segmented through the use of privileged access controls or multi-factor authentication. OPM's failure to implement such tiered identity management controls for system administrators exposed hundreds of its sub-networks, instead of a single sub-network, to breach. Had OPM implemented such controls, as required by OMB Memorandum M-11-11, the intrusion would have been detected earlier and the cyber thieves prevented from accessing the entire OPM network.

F. Announcements of the OPM Breaches

138. On June 4, 2015, OPM announced the October 2014 breach. OPM disclosed that the breach had resulted in the exposure and theft of the GII of approximately 4.2 million current, former, and prospective federal employees and contractors.

139. On June 12, 2015, OPM announced that the scope of the incident was broader than it had initially disclosed and that the GII of as many as 14 million current, former, and prospective federal employees and contractors had likely been exposed and stolen.

140. On July 9, 2015, OPM announced that the GII of approximately 21.5 million people had been exposed and stolen in the May 2014 breach. OPM disclosed that, of these compromised records, 19.7 million concerned individuals who had undergone federal background checks. OPM also disclosed that some of these records contained findings from interviews

conducted by background investigators, as well as approximately 1.1 million fingerprints. OPM stated that the remaining 1.8 million compromised records concerned other individuals: mostly job applicants' spouses, children, and other cohabitants.

141. On September 23, 2015, OPM announced that it had underestimated the number of compromised fingerprints, and that approximately 5.6 million fingerprints had been exposed and stolen in the cyberattacks on its systems.

142. Prior to OPM's announcements of the Data Breaches, Plaintiffs and Class members lacked notice that their GII might have been the subject of an unauthorized disclosure. Prior to these announcements, Plaintiffs and Class members did not have a reasonable basis to suspect or believe that such an unauthorized disclosure had occurred. Plaintiffs and Class members only learned that their GII had in fact been compromised when they subsequently received written notification from OPM.

G. What the Compromised Records Contain

143. The records taken in the Data Breaches are of the utmost sensitivity. Their theft violates the privacy rights and compromises the safety of tens of thousands of individuals, including covert intelligence agents.

144. Highly sensitive personal information was exposed and stolen in the Data Breaches. Among the compromised information:

• Residency details and contact information;

• Marital status and marital history;

• Private information about children, other immediate family members, and relatives;

• Information about financial accounts, debts, bankruptcy filings, and credit ratings and reports;

• Identities of past sexual partners;

• Findings from interviews conducted by background check investigators;

• Character and conduct of individuals as reported by references;

• Social Security numbers and birthdates of applicants and their spouses, children, and other cohabitants;

• Educational and employment history;

• Selective service and military records;

• Identities of personal and business acquaintances;

• Foreign contacts, including with officials and agents of foreign governments;

• Foreign travel and activities;

• Passport information;

• Psychological and emotional health information;

• Responses to inquiries concerning gambling compulsions, marital troubles, and past illicit drug and alcohol use;

• Police and arrest records;

• Association records;

• Investigations and clearance records;

• Information relating to criminal and non-criminal legal proceedings; and

• Financial and investment records.

145. The Electronic Official Personnel Folders stolen in the OPM Breaches include employee performance records, employment history, employment benefits information, federal job applications, resumes, school transcripts, documentation of military service, and birth certificates.

146. Stolen federal job applications and investigation forms contain, among other information, Social Security numbers, birthdates, birthplaces, other names used, mailing addresses, and financial records that include bank account and credit card information.

147. Also stolen was so-called adjudication information that federal investigators gather on those who apply for positions requiring heightened security clearance, such as positions in intelligence services. Adjudication information includes the results of polygraph examinations and the details of previous confidential work, as well as intimate personal facts. Exposure of this information imperils the safety of those who work covertly to protect American interests around the world.

H. OPM Remedial Measures

148. Following the Data Breaches, OPM notified people whose GII was compromised and offered them free identity theft protection services for a limited period of time. Specifically, OPM emailed federal employees whose GII was compromised, offering identity theft protection services via a link in the email. After some federal employees received unauthorized duplicates of these notification emails with false links that asked them to divulge personal information, OPM stopped sending notifications by email, and began sending paper notifications in the mail.

i. The Services Being Offered

149. OPM hired CSID and ID Experts—companies specializing in fraud resolution and identity theft protection—to provide services to individuals affected by the OPM Breaches.

150. At a combined cost of approximately $154 million, these companies agreed to provide victims with fraud monitoring and identity theft protection, insurance, and restoration services for either 18 months or three years, depending on the amount and sensitivity of the compromised GII.

151. OPM refers data breach victims who wish to receive additional protection to identitytheft.gov, a website managed by the FTC. That website recommends that individuals with compromised Social Security numbers purchase a credit freeze to ensure that no one can pull or modify a credit report. A credit freeze typically costs between $5 and $15. This remedial option is not included in the package being offered by OPM.

ii. OPM's Post-Breach Cybersecurity Measures Leave OPM's Systems Exposed to Further Attack

152. 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." The IG found that OPM had followed less than half of the recommendations in the 2013 and 2014 audits, and that 21 of the 27 recommendations in the 2015 audit had been outstanding for at least a year. The IG noted that its recommendations garnered little attention even when they were repeated year after year and accompanied by warnings that OPM's failures to act magnified the risk of a data breach.

153. The IG found in November 2015 that OPM's management of its systems authorization program had regressed and would continue to be classified as a material weakness. The IG determined that up to 23 major OPM information systems were operating without a valid authorization, whereas there were eleven such systems in 2014. The IG stated 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."

154. In its 2015 audit, the IG again recommended that OPM shut down information systems operating without valid authorizations. OPM again refused, and it continues to operate information systems that lack valid authorizations.

155. The IG further found in November 2015 that OPM continued to lack a mature continuous monitoring program and that the security controls for its newly installed monitoring program had not been appropriately tested. On a scale of 1 to 5, with 1 being the least effective, the IG found that OPM's continuous monitoring program was functioning at level 1—"Ad-Hoc."

156. With regard to multi-factor authentication, the IG found in November 2015 that while OPM required multi-factor authentication for laptops and other devices connecting to OPM's systems, none of OPM's major applications required multi-factor authentication as required by OMB Memorandum M-11-11.

157. The IG's November 2015 audit also reported a continuing failure by OPM to provide adequate security training to many individuals responsible for the security of the information under OPM's control.

iii. Post-Breach Changes in OPM's Leadership Leave OPM without a Chief Information Officer and a Director Authorized to Act

158. On July 10, 2015, Katherine Archuleta, Director of OPM, resigned.

159. Also on July 10, 2015, the President appointed Beth F. Cobert—then the Deputy Director for Management of the Office of Management and Budget—to serve as Acting Director of OPM. On November 10, 2015, the President appointed Cobert to serve as Director of OPM.

160. On February 10, 2016, the IG informed Cobert that the Federal Vacancies Reform Act prohibits her from serving as Acting Director of OPM, because she was never a "first assistant" to the Director of OPM. 5 U.S.C. § 3345(b).

161. The IG further informed Cobert that, under 5 U.S.C. § 3348(d), any actions taken by her since her nomination are void and may not be subsequently ratified. The IG stated that "these actions may be open to challenges before the federal district court for the District of Columbia."

162. On February 22, 2016, two days before she was scheduled to testify before the House Committee on Oversight and Government Reform, Donna Seymour, Chief Information Officer of OPM, resigned. As of this filing, a replacement has not been appointed.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

163. As a result of Defendants' violations of law, Plaintiffs and Class members have sustained and will continue to sustain economic loss and other harm. They have experienced and/or face an increased risk of experiencing the following forms of injuries:
A. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of GII, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards;

B. money and time lost as a result of fraudulent access to and use of their financial accounts, some of which accounts were

never reimbursed;

C. loss of use of and access to their financial accounts and/or credit;

D. diminished prospects for future employment and/or promotion to positions with higher security clearances as a result of their GII having been compromised;

E. money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;

F. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

G. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

H. money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns, including by completing paperwork associated with the reporting of fraudulent returns and the manual filing of replacement returns;

I. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches, including efforts to research how to prevent, detect, contest, and recover from misuse of GII;

J. anticipated future costs from the purchase of credit monitoring and identity theft protection services once the temporary services being offered by OPM expire;

K. loss of the opportunity to control how their GII is used;

L. continuing risks from the unmasking of confidential identities; and

M. continuing risks to their GII and that of their family members, friends, and associates, which remains subject to further harmful exposure and theft as long as OPM fails to undertake appropriate, legally required steps to protect the GII in its possession.

VI. CLASS ACTION ALLEGATIONS

164. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), and/or (b)(1), (b)(2), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

165. The proposed Class is defined as:

> All current, former, and prospective employees of the federal government and its contractors, and their family members and cohabitants, whose sensitive personal information was compromised as a result of the breaches of OPM's electronic information systems in 2014 and 2015 or the breach of KeyPoint's electronic information systems in 2013 and 2014.

The proposed Questionnaire Subclass is defined as:

> All Class members who submitted SF-85, SF-85P, or SF-86 forms.

The proposed KeyPoint Subclass is defined as:

> All Class members who were the subject of KeyPoint investigations.

Excluded from the proposed Class and Subclasses are:

a. Senior officers, officials, and executives of Defendants and their immediate family members; and

b. Any judicial officers to whom this case is assigned and their respective staffs.

Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into further subclasses, or modified in any other way.

Numerosity and Ascertainability

166. The size of the Class can be estimated with reasonable precision, and the number is great enough that joinder is impracticable.

167. The number of Class members is in the millions. The disposition of their claims in a single action will provide substantial benefits to all parties and to the Court.

168. Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants. Notice of this action can be readily provided to the Class.

Typicality

169. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised in the Data Breaches.

Adequacy of Representation

170. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class members.

Predominance of Common Issues

171. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:
(a) Whether OPM, in violation of the Privacy Act, failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats to their security and integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members;

(b) Whether OPM, in violation of the Privacy Act, disclosed Plaintiffs' and Class members' GII without their prior written consent for no statutorily permitted purpose;

(c) Whether OPM's decisions not to follow the IG's directions concerning FISMA requirements for information security constitute intentional or willful violations;

(d) Whether OPM entered into, and breached, contracts with Plaintiffs and Questionnaire Subclass members to properly safeguard their GII;

(e) Whether OPM's conduct violated the Administrative Procedure Act and, if so, what equitable remedies should issue;

(f) Whether KeyPoint owed, and breached, duties to Plaintiffs and Class members to implement reasonable and adequate cybersecurity measures and to promptly alert them if their GII was compromised;

(g) Whether KeyPoint acted negligently in failing to disclose, and falsely representing, material facts relating to its cybersecurity precautions;

(h) Whether KeyPoint's cybersecurity failures and their proximate results are highly offensive to a reasonable person in Plaintiffs' and Class members' position;

(i) Whether KeyPoint violated FCRA and, if so, what statutory remedies should issue;

(j) Whether KeyPoint engaged in unfair or deceptive acts or practices in the course of its business;

(k) Whether KeyPoint entered into, and breached, contracts with Plaintiffs and KeyPoint Subclass members to properly safeguard their GII; and

(l) Whether Plaintiffs and Class members are entitled to damages and declaratory and injunctive relief.

Superiority

172. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class members' claims, it is likely that few, if any, Class members could afford to seek redress for Defendants' violations.

173. Class treatment of common questions of law and fact would also be a superior method to piecemeal litigation in that class treatment will conserve the resources of the courts and will promote consistency and efficiency of adjudication.

174. Classwide declaratory, equitable, and injunctive relief is appropriate under Rule 23(b)(1), (b)(2), and/or (c)(4) because Defendants have acted on grounds that apply generally to the Class, and inconsistent adjudications would establish incompatible standards and substantially impair the ability of Class members and Defendants to protect their respective interests. Classwide relief assures fair, consistent, and equitable treatment of Class members and Defendants.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

(Against OPM)

Violations of the Privacy Act of 1974, 5 U.S.C. § 552a

175. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

176. OPM is an agency within the meaning of the Privacy Act.

177. OPM obtained and preserved Plaintiffs' and Class members' GII, including GII contained in SF-85, SF-85P, and SF-86 forms, in a system of records.

178. In violation of the Privacy Act, OPM willfully and intentionally failed to comply with FISMA. OPM's violations of federal law adversely affected Plaintiffs and Class members. Despite known and persistent threats from cyberattacks, OPM allowed multiple "material weaknesses" in its information security systems to continue unabated. As a result, Plaintiffs' and Class members' GII under OPM's control was exposed, stolen, and misused.

179. IG reports repeatedly warned OPM officials that OPM's systems were highly vulnerable to cyberattacks and not in compliance, in several specific ways, with the Privacy Act, FISMA, and other rules and regulations governing cybersecurity at OPM. OPM officials knew that these warnings were well-founded: among other things, OPM suffered successful cyberattacks in 2009 and 2012. OPM officials were also aware that each month saw more than 10 million attempted electronic incursions against its information systems. OPM officials, however, decided not to take adequate, legally required measures to protect the data with which the agency had been entrusted.

180. OPM was required—but failed—to take many steps to comply with controlling information security rules and regulations. OPM declined to implement PIV multi-factor authentication for all 47 of its major applications, as required by OMB Memorandum M-11-11 and as stated in the IG's audit reports. OPM affirmatively refused to shut down faulty systems even after the IG notified OPM that it was required to do so under FISMA. OPM's violations of applicable federal law include its willful failures to ensure that all operating software systems receive valid authorizations; to centralize its cybersecurity structure to provide effective management of its information systems; to monitor those systems continuously and create internal firewalls to limit the adverse effects of a breach; and to adequately train its employees responsible for cybersecurity. OPM intentionally disregarded IG findings that each of these failures rendered the agency not in compliance with federal requirements.

181. In violation of the Privacy Act and FISMA, OPM intentionally failed to comply with many other standards promulgated under 40 U.S.C. § 11331, including with regard to risk and configuration management, incident response and reporting, contractor systems, security capital planning, and contingency planning. OPM's actions were calculated to downplay the scope of the OPM Breaches and to preserve data accessibility to the detriment of data confidentiality and integrity. OPM did not destroy GII where permitted, and allowed GII to be accessible to unauthorized third parties.

182. In a continuous course of wrongful conduct, OPM willfully refused to implement electronic security safeguards required by law. OPM willfully failed 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, in violation of 5 U.S.C. § 552a(e)(10).

183. As a direct and proximate result of its non-compliance with federal requirements and its intentional disregard of the IG's findings under FISMA, OPM willfully disclosed Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose, in violation of 5 U.S.C. § 552a(b).

184. OPM's willful and intentional violations of federal law continue. OPM has failed to undertake compulsory security precautions to safeguard Plaintiffs' and Class members' GII.

185. Plaintiffs and Class members have sustained and will continue to sustain actual damages and pecuniary losses directly traceable to OPM's violations set forth above. Plaintiffs and Class members are entitled to damages under 5 U.S.C. §§

552a(g)(1)(D) and (g)(4).

SECOND CLAIM FOR RELIEF

(Against the United States)

Breach of Contract within the Little Tucker Act, 28 U.S.C. § 1346(a)

186. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

187. Plaintiffs bring this cause of action on behalf of the Questionnaire Subclass.

188. Plaintiffs and Questionnaire Subclass members entered into valid and binding contracts with OPM.

189. OPM offered to ensure the confidentiality of Plaintiffs' and Questionnaire Subclass members' sensitive personal information in exchange for their submission of information needed by the government to conduct investigations. The SF-85, SF-85P, and SF-86 forms state that the government derives the benefit from this exchange of, among other things, being able to conduct background investigations, reinvestigations, and/or continuous evaluations of persons under consideration for, or under consideration for retention of, federal government or contractor positions, or of persons requiring eligibility for access to classified information.

190. Plaintiffs and Questionnaire Subclass members agreed to provide their sensitive personal information in return for the opportunity to be considered for government employment opportunities. Plaintiffs and Questionnaire Subclass members agreed to provide their sensitive personal information on the condition and with the reasonable understanding that—as stated in the SF-85, SF-85P, and SF-86 forms—"the information will be protected from unauthorized disclosure." OPM promised not to disclose such information without their consent, except for eleven enumerated "routine uses" and as permitted by the Privacy Act. Plaintiffs and Questionnaire Subclass members accepted the government's offer, by providing their sensitive personal information to the government in SF-85, SF-85P, or SF-86 forms.

191. At all relevant times, the agents and representatives of OPM had actual authority to act on behalf of OPM and to bind the United States. Federal statutes, agency regulations, and executive orders conferred authority on OPM to obtain this information.

192. A contract existed between OPM and Plaintiffs and Questionnaire Subclass members. When they provided their sensitive personal information to OPM, Plaintiffs and Questionnaire Subclass members reasonably expected and understood that OPM was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes, and that OPM had the authority to enter into the agreement to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes. But for this expectation and understanding, Plaintiffs and Questionnaire Subclass members would not have provided their sensitive personal information to OPM.

193. OPM did not perform on its promises to protect Plaintiffs' and Questionnaire Subclass members' sensitive personal information from unauthorized disclosure and not to disclose it for non-routine use absent their consent. Instead, in breach of its express and implied contractual obligations, OPM failed to protect Plaintiffs' and Questionnaire Subclass members' sensitive personal information from unauthorized disclosure for improper purposes.

194. OPM's breach of contract injured Plaintiffs and Questionnaire Subclass members. They are entitled to damages in an amount to be proven at trial.

195. In connection with this claim, Plaintiffs and Questionnaire Subclass members waive the right to recovery in excess of $10,000 per person.

THIRD CLAIM FOR RELIEF

(Against OPM)

Violations of the Administrative Procedure Act, 5 U.S.C. § 701, *et seq.* ("APA")

196. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

197. The APA provides for judicial review of agency actions causing legal harm or adverse effects to a plaintiff. 5 U.S.C. § 702. The APA requires the Court to deem unlawful and set aside agency actions, findings, and conclusions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). The APA also requires the Court to compel agency action that has been unlawfully withheld or unreasonably delayed. 5 U.S.C. § 706(1).

198. As documented in the IG's annual audit reports, OPM acted arbitrarily and capriciously, abused its discretion, and violated the Privacy Act, FISMA, and regulations and technical standards for data security issued by the Office of Management and Budget ("OMB") and the National Institute for Standards and Technology ("NIST") that FISMA makes "compulsory and binding" on OPM.

199. Continuing to violate the APA, OPM still has not adopted or implemented a data security plan that satisfies these requirements.

200. Final agency actions of OPM prior to the OPM Breaches that were arbitrary, capricious, an abuse of discretion, and violative of applicable federal provisions and standards include OPM's decisions to:

a. operate computer and software systems without valid authorizations;

b. operate computer and software systems without requiring multi-factor authentication to access them;

c. operate computer and software systems without implementing adequate network and data segmentation;

d. operate computer and software systems without implementing layered security defenses, such as firewalls and host level anti-malware;

e. operate computer and software systems without adequately and continuously monitoring security controls and their effectiveness;

f. elect not to encrypt sensitive personal information under its control;

g. rely on a decentralized structure for governance and management of information security;

h. provide its employees with inadequate training in electronic security techniques, defenses, and protocols; and

i. operate without a comprehensive inventory of its servers, databases, and network devices.

201. The above decisions resulted from a consummation of OPM's decision making process. Judicial review is the only adequate mechanism available to correct them.

202. Final agency actions of OPM subsequent to the OPM Breaches that were arbitrary, capricious, an abuse of discretion, and violative of applicable federal requirements and standards include OPM's decisions not to:

a. shut down or otherwise isolate the compromised electronic systems;

b. undertake measures to identify, disrupt, or limit the ongoing attacks on its systems; and

c. change the access codes used to gain entry into its systems.

203. The above decisions resulted from a consummation of OPM's decision making process. Judicial review is the only adequate mechanism available to correct them.

204. OPM is under an affirmative legal obligation to promulgate and implement a data security plan that meets the standards and requirements of FISMA. In its annual audits, the IG repeatedly instructed OPM to bring its information systems into compliance with FISMA. Each year, OPM chose not to do so. For example, from 2011 to 2014, the IG advised OPM that it was not in compliance with FISMA because of its decentralized cybersecurity governance structure. OPM failed to centralize its cybersecurity governance or to otherwise bring its systems into compliance.

205. The IG audit released in November 2015 determined that OPM's cybersecurity is deficient and violative of FISMA. The IG reported, among other things, that an outbound web proxy is still missing at OPM, that controls have not been implemented to prevent unauthorized devices from connecting to the OPM network, that OPM's vulnerability management program remains substandard, and that a number of deficiencies previously identified by the IG as prone to exploitation by cyber thieves still exist within OPM.

206. OPM's current information security measures do not comply with the Privacy Act, FISMA, or the regulations and technical standards issued by the OMB and the NIST that FISMA makes "compulsory and binding" on OPM. In consequence, Plaintiffs' and Class members' GII remains at imminent risk of being exposed and stolen.

207. Plaintiffs and Class members are entitled to judicial review of OPM's actions because they have suffered legal wrongs, have been adversely affected, and remain aggrieved by OPM's final actions for which there is no other adequate remedy. Declaratory relief is warranted under 5 U.S.C. § 706(2)(A) and injunctive relief under 5 U.S.C. § 706(1).

FOURTH CLAIM FOR RELIEF

(Against OPM and KeyPoint)

Declaratory Judgment and Injunctive Relief

208. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

209. Based on Defendants' violations of law described herein, equitable relief is warranted under (i) the APA provisions referenced above, (ii) the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, (iii) the common laws and statutory provisions that KeyPoint violated, and (iv) this Court's inherent authority to order equitable remedies for unlawful actions and inactions.

210. Defendants' failure to protect the GII of Plaintiffs and Class members abridged their privacy rights, resulted in concrete economic injuries, and placed millions of government workers at a heightened risk of identity theft, fraud, and other detrimental consequences.

211. Notwithstanding the IG's November 2015 identification of continuing material weaknesses and legal violations in OPM's information security protocols, OPM has not taken adequate, compulsory actions to protect Plaintiffs' and Class members' GII. OPM's continuing failure in these respects creates a substantial risk of imminent further harm to Plaintiffs, Class members, and others.

212. OPM's ongoing failure to secure its information systems and to protect the GII of current, former, and prospective federal government employees and contractors, is harmful to the public interest. The Data Breaches, and OPM's failure to properly respond to them, create a disincentive to those considering government service. By compromising the integrity of

the clearance process, and by exposing the confidential information of those in sensitive government positions, OPM's unlawfully lax data security has harmed, and creates a substantial risk of further harm to, the national security of the United States. OPM's unlawfully lax data security has also led to the filing of numerous false tax returns and will continue to impose costs on the Internal Revenue Service, including by impeding its ability to collect taxes accurately and efficiently.

213. Plaintiffs seek a declaratory judgment finding unlawful the relevant conduct of Defendants and requiring them to indemnify and hold harmless any Class member who has sustained or will sustain economic injury as a result of the Data Breaches.

214. Plaintiffs further seek an injunction requiring Defendants to extend free lifetime identity theft protection services, including credit monitoring and identity theft insurance, to Plaintiffs and the Class.

215. Plaintiffs also seek an injunction requiring OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA, by, among other things, mandating that all unauthorized information systems be shut down and validly authorized before being reactivated.

FIFTH CLAIM FOR RELIEF

(Against KeyPoint)

Negligence

216. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

217. It was reasonably foreseeable to KeyPoint that a breach of its information systems could occur and cause harm by compromising the GII of current, former, and prospective federal government employees. KeyPoint's and OPM's electronic systems were linked, shared, and overlapping. It was reasonably foreseeable that a breach of KeyPoint's systems would expose OPM's systems, and the GII contained therein, to a successful cyberattack.

218. KeyPoint owed a duty of care to Plaintiffs and Class members to adequately protect their GII—both in KeyPoint's network and in OPM's network—and the security credentials that could be used to access that GII. More specifically, with regard to Plaintiffs and Class members, KeyPoint was obligated to:

a. exercise due and reasonable care in obtaining, retaining, securing, protecting, and deleting GII in KeyPoint's possession;

b. exercise due and reasonable care in providing, securing, protecting, and deleting the security credentials for accessing GII on KeyPoint's and OPM's systems;

c. exercise due and reasonable care in expanding its workforce by, among other things, performing due diligence of candidates who, if hired, would have access to GII and appropriately supervising new hires;

d. safeguard GII through security procedures, protocols, and systems that are reasonable, adequate, and in conformance with recognized data security industry standards; and

e. implement procedures and protocols to promptly detect, record, mitigate, and notify the victims of data breaches.

219. KeyPoint's duties in these respects applied to Plaintiffs and Class members because they were the reasonably foreseeable victims of breaches of its information systems. KeyPoint collected and stored Plaintiffs' and Class members' GII in the course of conducting background and security clearance investigations. KeyPoint knew or should have known of the risks inherent in collecting and storing GII and the crucial importance of adequate data security, including to protect the access credentials relied on to perpetrate the Data Breaches.

220. KeyPoint owed similar duties of care to Plaintiffs and Class members under FCRA and state statutes requiring KeyPoint to reasonably safeguard Plaintiffs' and Class members' GII and to promptly notify them of any breach thereof.

221. KeyPoint's duties of care also arose from the special relationship between KeyPoint and those who entrusted it with their sensitive personal information. Plaintiffs and KeyPoint Subclass members permitted KeyPoint to access such information with the expectation that KeyPoint would take reasonable and effective precautions to protect such information from disclosure to unauthorized third parties and/or for improper purposes.

222. KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to access it on KeyPoint's and OPM's systems. KeyPoint's information security defenses did not conform to recognized industry standards.

223. KeyPoint's acts and omissions created a foreseeable risk of harm to Plaintiffs and Class members, breaching the duties of care it owed them. KeyPoint's breached its duties by failing 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.

224. KeyPoint also breached its duties to Plaintiffs and Class members by failing to cause them to be promptly notified that their GII had been compromised. The KeyPoint Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

225. But for KeyPoint's wrongful and negligent breaches of its duties of care, Plaintiffs' and Class members' GII would not have been compromised or they would have mitigated their damages more effectively.

226. Had KeyPoint promptly caused Plaintiffs and Class members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of GII misuse. Additionally, those whom KeyPoint began to investigate after its systems had been breached could have declined to provide their sensitive personal information to KeyPoint.

227. Plaintiffs and Class members sustained harm as a result of KeyPoint's negligence in failing to prevent and to timely cause them to be notified of the KeyPoint Breach.

228. Plaintiffs and Class members sustained harm as a result of KeyPoint's negligence in failing to protect and secure its user log-in credentials. KeyPoint's negligence in failing to protect and secure its user log-in credentials was a substantial factor in causing the Data Breaches.

229. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

SIXTH CLAIM FOR RELIEF

(Against KeyPoint)

Negligent Misrepresentation and Concealment

230. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

231. KeyPoint owed a duty to communicate to Plaintiffs and Class members all facts within its actual or constructive knowledge that were material to KeyPoint's investigatory services as they affected Plaintiffs' and Class members' rights and interests.

232. KeyPoint breached this duty by concealing from Plaintiffs and Class members that its information security systems did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to improperly access it on KeyPoint's and on OPM's systems.

233. KeyPoint knew or should have known that its information security systems did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to improperly access it on KeyPoint's and OPM's systems.

234. These concealed facts were material to KeyPoint's investigatory services as they affected Plaintiffs' and Class members' rights and interests. A reasonable person in Plaintiffs' and Class members' position would expect to be notified of these facts.

235. Plaintiffs and Class members were unaware of, and had no reasonable means of discovering, these concealed facts.

236. KeyPoint falsely represented to Plaintiffs and Class members that all of its electronic systems are secure from unauthorized access and that it "maintains a secure network to safeguard consumer information from internal and external threat." KeyPoint knew or should have known that these representations were false.

237. By suppressing and misrepresenting material facts known to it alone, KeyPoint misled Plaintiffs and Class members in violation of law. 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. Had KeyPoint disclosed the inadequacy of its security measures, Plaintiffs and Class members would have taken steps to prevent their injuries and/or to mitigate their damages more effectively.

238. Plaintiffs and Class members sustained economic loss as a direct and proximate result of KeyPoint's negligent misrepresentation and concealment of material facts, and are entitled to corresponding damages.

SEVENTH CLAIM FOR RELIEF

(Against KeyPoint)

Invasion of Privacy

239. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

240. Plaintiffs and Class members reasonably expected that their GII would be kept private and secure, and would not be disclosed to any unauthorized third party and/or for any improper purpose.

241. KeyPoint unlawfully invaded Plaintiffs' and Class members' privacy rights by:

a. failing to adequately secure their GII, and the user log-in credentials relied on to breach its and OPM's systems, from disclosure to unauthorized third parties for improper purposes;

b. disclosing personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. disclosing personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

242. In failing to adequately secure Plaintiffs' and Class members' GII, KeyPoint acted in reckless disregard of their privacy rights. KeyPoint knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' and Class members' position.

243. KeyPoint violated Plaintiffs' and Class members' right to privacy under the common law as well as under the California Constitution, Article I, Section 1.

244. As a direct and proximate result of KeyPoint's unlawful invasions of privacy, Plaintiffs' and Class members' reasonable expectations of privacy were frustrated and defeated. KeyPoint's unlawful invasions of privacy damaged Plaintiffs and Class members as set forth above, and they are entitled to appropriate relief.

EIGHTH CLAIM FOR RELIEF

(Against KeyPoint)

Violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA")

245. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

246. KeyPoint recognizes in its Privacy Policy that it is a consumer reporting agency and, as such, is required by FCRA to maintain the confidentiality of all consumer information. KeyPoint is a consumer reporting agency under FCRA because, for monetary fees, it regularly engages in the practice of assembling and evaluating consumer credit information for the purpose of furnishing consumer reports to third parties (such as OPM). 15 U.S.C. § 1681a(f). KeyPoint's standard background and security clearance check procedure entails searching and analyzing the records of commercial credit reporting agencies.

247. As individuals, Plaintiffs and Class members are consumers entitled to the protections of FCRA. 15 U.S.C. § 1681a(c).

248. KeyPoint willfully violated FCRA.

249. In violation of 15 U.S.C. § 1681b(a)(3), consumer reports concerning Plaintiffs and Class members were furnished by or from KeyPoint for no statutorily permitted purpose.

250. In violation of 15 U.S.C. § 1681e(a), KeyPoint failed to maintain reasonable procedures to limit the furnishing of consumer reports to statutorily permitted purposes, in at least the following respects:

a. KeyPoint failed to undertake reasonable electronic security precautions that would have prevented the KeyPoint Breach and its unauthorized furnishing of consumer reports;

b. KeyPoint furnished consumer reports to OPM despite KeyPoint's actual or constructive knowledge of its and OPM's inadequate electronic security precautions; and

c. KeyPoint failed to undertake reasonable electronic security precautions to protect the user log-in credentials used to

commit the Data Breaches, and this failure caused consumer reports to be furnished for no statutorily permitted purpose.

251. KeyPoint's violations of FCRA directly and proximately caused the exposure, theft, and misuse of Plaintiffs' and Class members' GII. Their GII stored on KeyPoint's network was compromised in the KeyPoint Breach. KeyPoint user log-in credentials were used to hack into OPM's information systems and to compromise Plaintiffs' and Class members' GII stored on OPM's network. KeyPoint's failure to secure its user log-in credentials was a substantial factor in causing the Data Breaches.

252. As a direct and proximate result of KeyPoint's violations of FCRA, Plaintiffs and Class members have sustained damages as set forth above. They are entitled to their actual damages or statutory damages, as well as attorneys' fees and costs as may be permitted by statute.

NINTH CLAIM FOR RELIEF

(Against KeyPoint)

Violations of State Statutes Prohibiting Unfair and Deceptive Trade Practices

253. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

254. KeyPoint is engaged in trade and commerce. As relevant here, KeyPoint's acts, practices, and omissions occurred in the course of KeyPoint's business of conducting background and security clearance investigations of Plaintiffs and Class members throughout the United States.

255. KeyPoint's conduct as alleged herein constitutes unfair, deceptive, fraudulent, unconscionable, and/or unlawful acts or practices. Among other violations, KeyPoint:

a. failed to implement and maintain data security practices adequate to safeguard Plaintiffs' and Class members' GII and the security credentials used to breach its and OPM's information systems;

b. made misleading and deceptive representations and omissions in its publicly disseminated Privacy Policy regarding its ability and efforts to secure Plaintiffs' and Class members' GII;

c. failed to disclose that its data security practices and protocols were insufficient to protect Plaintiffs' and Class members' GII;

d. failed to timely disclose the KeyPoint Breach to Plaintiffs and Class members; and

e. continued to accept and store Plaintiffs' and Class members' GII even after obtaining actual or constructive notice of its security vulnerabilities.

256. By reason of its acts and omissions, KeyPoint violated the following statutes prohibiting unfair or deceptive acts or practices:

a. The California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq.*;

b. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

c. The Idaho Consumer Protection Act, Idaho Code Ann. § 48-603(18), *et seq.*;

d. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 505/2, *et seq.*, and the Illinois

Uniform Deceptive Trades Practices Act, 815 Ill. Comp. Stat. § 510/2(a)(12), *et seq.*;

e. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915, *et seq.*;

f. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2, *et seq.*;

g. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(17) & 57-12-3, *et seq.*;

h. The North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-1.1(a), *et seq.*;

i. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. §§ 201-2(4)(xxi) & 201-3, *et seq.*;

j. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(14), *et seq.*; and

k. The Washington Consumer Protection Act, Wash. Rev. Code Ann. § 19.86.020, *et seq.*

257. As a direct and proximate result of KeyPoint's violations of the above provisions, Plaintiffs and Class members sustained damages, as described herein, and are entitled to appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

258. Before filing this Complaint, counsel for Plaintiffs sent a copy of this Complaint to the Attorney General of Washington, pursuant to Wash. Rev. Code § 19.86.095.

TENTH CLAIM FOR RELIEF

(Against KeyPoint)

Violations of State Data Breach Acts

259. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

260. The KeyPoint Breach constitutes a security breach that triggered the requirements of various state data breach acts. The GII exposed and stolen in the KeyPoint Breach includes personal information protected by these statutes.

261. In violation of state data breach acts, KeyPoint unreasonably delayed in causing Plaintiffs and Class members to be notified of the KeyPoint Breach after KeyPoint knew or should have known of it. The KeyPoint Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

262. KeyPoint's failure to cause timely notice of the KeyPoint Breach to be provided violated the following statutes:
a. Cal. Civ. Code § 1798.80, *et seq.*;

b. Ga. Code Ann. § 10-1-912(a), *et seq.*;

c. 815 Ill. Comp. Stat. 530/10(a), *et seq.*;

d. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

e. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

f. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

g. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

h. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

i. Va. Code Ann. § 18.2-186.6(B), *et seq.*;

j. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*; and

k. Wis. Stat. Ann. § 134.98(2), *et seq.*

263. KeyPoint's violations of these statutes damaged Plaintiffs and Class members. Had KeyPoint timely caused Plaintiffs and Class members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of misuse of their sensitive personal information. Additionally, those whom KeyPoint began to investigate after its systems had been breached could have declined to provide their sensitive personal information to KeyPoint.

264. In further violation of Cal. Civ. Code § 1798.80, *et seq.*, KeyPoint failed to implement and maintain security measures sufficient to prevent the KeyPoint Breach and protect the security credentials used to perpetrate the Data Breaches. KeyPoint's violations of Cal. Civ. Code § 1798.80 damaged Plaintiffs and Class members.

265. KeyPoint failed to establish appropriate procedures to ensure the confidentiality of Plaintiffs' and Class members' medical information and to protect such information from unauthorized use and disclosure, in violation of Cal. Civ. Code § 56.20-56.245, *et seq.* KeyPoint also violated Wis. Stat. §§ 146.82 and 146.84 and Va. Code § 32.1-127.1:03(3) by disclosing Plaintiffs' and Class members' medical records without specific authorization or other justification. KeyPoint's violations of Cal. Civ. Code § 56.20-56.245, *et seq.*, Wis. Stat. §§ 146.82 and 146.84, and Va. Code § 32.1-127.1:03(3) damaged Plaintiffs and Class members.

266. Based on KeyPoint's violations of the foregoing provisions, Plaintiffs and Class members are entitled to appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

ELEVENTH CLAIM FOR RELIEF

(Against KeyPoint)

Breach of Contract

267. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

268. Plaintiffs bring this cause of action on behalf of the KeyPoint Subclass.

269. Plaintiffs and KeyPoint Subclass members entered into valid and binding contracts with KeyPoint.

270. 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 clearance investigations. KeyPoint derived the benefit from this exchange of, among other things, being able to conduct such investigations and receiving associated payments from OPM.

271. Plaintiffs and Class members agreed to furnish their sensitive personal information to KeyPoint, or to permit KeyPoint to access it, in return for the opportunity to be considered for government employment opportunities. Plaintiffs and Class members agreed to permit KeyPoint to access their sensitive personal information on the condition that KeyPoint would act

to "secure" such information "from unauthorized access." Since October 2012 at the latest, KeyPoint continuously promised to "maintain[] a secure network to safeguard consumer information from internal and external threat." Plaintiffs and Class members accepted KeyPoint's offer, by permitting KeyPoint to access their sensitive personal information.

272. At all relevant times, the agents and representatives of KeyPoint had actual authority to act on behalf of, and to bind, KeyPoint.

273. A contract existed between KeyPoint and Plaintiffs and KeyPoint Subclass members. When they permitted KeyPoint to access their sensitive personal information, Plaintiffs and KeyPoint Subclass members reasonably expected and understood that KeyPoint was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes, and that KeyPoint's agents and representatives had the authority to enter into this agreement to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes. But for this expectation and understanding, Plaintiffs and KeyPoint Subclass members would not have permitted KeyPoint to access their sensitive personal information.

274. KeyPoint did not perform on its promises to safeguard Plaintiffs' and KeyPoint Subclass members' sensitive personal information and to maintain a secure network. Instead, in breach of its express and implied contractual obligations, KeyPoint failed to undertake reasonable and appropriate security precautions. The proximate result was the KeyPoint Breach and the theft of user log-in credentials used to perpetrate the Data Breaches.

275. KeyPoint's breach of contract injured Plaintiffs and KeyPoint Subclass members. They are entitled to damages in an amount to be proven at trial.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek a judgment against Defendants through an Order:

A. certifying this case as a class action, designating Plaintiffs as Class and Subclass representatives, and appointing Plaintiffs' counsel to represent the Class;

B. finding Defendants liable for their failure to establish adequate and legally required safeguards to ensure the security of Plaintiffs' and Class members' GII compromised in the Data Breaches;

C. requiring Defendants to pay money damages, including actual and statutory damages, to Plaintiffs and Class members;

D. declaring that the relevant conduct of Defendants is unlawful and that Defendants shall indemnify and hold harmless any Class member who has sustained or will sustain economic injury as a result of the Data Breaches;

E. enjoining Defendants to extend free lifetime identity theft and fraud protection services, including credit monitoring and identity theft insurance, to Plaintiffs and the Class;

F. enjoining OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA, by, among other things, mandating that all unauthorized information systems be shut down and validly authorized before being reactivated;

G. awarding reasonable attorneys' fees and costs as may be permitted by law;

H. awarding pre-judgment and post-judgment interest as may be prescribed by law; and

I. granting such further and other relief as may be just and proper.

IX. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: March 14, 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

Peter A. Patterson

Harold Reeves

COOPER & KIRK, PLLC

1523 New Hampshire Avenue, N.W.

Washington, D.C. 20036

Tina Wolfson

Theodore Maya

Bradley King

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

STUEVE SIEGEL HANSON LLP

460 Nichols Road, Suite 200

Kansas City, MO 64112

Denis F. Sheils

KOHN, SWIFT & GRAF, P.C.

One South Broad Street, Suite 2100

Philadelphia, PA 19107

Graham B. LippSmith

KASDAN LIPPSMITH WEBER TURNER LLP

500 South Grand Avenue, Suite 1310

Los Angeles, CA 90071

Nicholas Koluncich III

THE LAW OFFICES OF NICHOLAS KOLUNCICH III

500 Marquette Avenue N.W., Suite 1200

Albuquerque, NM 87102

Edward W. Ciolko

KESSLER TOPAZ MELTZER & CHECK LLP

280 King of Prussia Road

Radnor, PA 19087

Steven W. Teppler

ABBOTT LAW GROUP, P.A.

2929 Plummer Cove Road

Jacksonville, FL 32223

Plaintiffs' Counsel