NOT YET SCHEDULED FOR ORAL ARGUMENT

United States Court of Appeals
for the District of Columbia Circuit

No. 19-7020

CHANTAL ATTIAS, Individually and on behalf of all others similarly situated; RICHARD BAILEY, Individually and on behalf of all others similarly situated; LATANYA BAILEY, Individually and on behalf of all others similarly situated; LISA HUBER, Individually and on behalf of all others similarly situated; ANDREAS KOTZUR, Individually and on behalf of all others similarly situated; CURT TRINGLER, Individually and on behalf of all others similarly situated; and CONNIE TRINGLER, Individually and on behalf of all others similarly situated,

Plaintiffs – Appellants,

v.

CAREFIRST, INC., doing business as Group Hospitalization and MEDICAL SERVICES, INC., doing business as CareFirst of Maryland, Inc., doing business as Carefirst BlueCross BlueShield, doing business as CareFirst BlueChoice, Inc.; GROUP HOSPITALIZATION AND MEDICAL SERVICES, INC., doing business as Carefirst BlueCross BlueShield, doing business as CareFirst BlueChoice, Inc.; CAREFIRST BLUECHOICE, INC., doing business as Carefirst BlueCross BlueShield, doing business as Group Hospitalization and Medical Services, Inc., doing business as CareFirst of Maryland, Inc.; and CAREFIRST OF MARYLAND, INC., doing business as Carefirst BlueCross BlueShield, doing business as BlueCross and BlueShield of Maryland Inc., doing business as CareFirst BlueChoice, Inc.,

Defendants – Appellees.

On Appeal from the United States District Court for the District of Columbia in Case no. 1:15-cv-00882-CRC, Beryl A. Howell, Judge.

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

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to the Circuit Rule 28, Appellants state the following:

1. Parties and Amici

Plaintiffs-Appellants:	Chantal Attias, Individually and on behalf of all other similarly situated
	Andreas Kotzur, Individually and on behalf of all others similarly situated
	Richard Bailey, Individually and on behalf of all others similarly situated
	Latanya Bailey, Individually and on behalf of all others similarly situated
	Curt Tringler, Individually and on behalf of all others similarly situated
	Connie Tringler, Individually and on behalf of all others similarly situated
	Lisa Huber, Individually and on behalf of all others similarly situated
Defendants-Appellees:	CareFirst, Inc.
	Group Hospitalization and Medical Services, Inc.
	CareFirst of Maryland, Inc.
	CareFirst BlueChoice

2. Rulings under Review

The Plaintiffs are appealing from the Order and supporting memorandum opinion of District Judge Christopher R. Cooper entered on January 30, 2019, granting in part and denying in part CareFirst's Motion to Dismiss for failure to state

a claim. App. 123-138.[1] On February 26, 2019, the district court entered Final Judgment pursuant to Federal Rule of Civil Procedure 54(b) finding "that there is 'no just reason for delay' of entry of final judgment as to Counts I through XI for Plaintiffs Chantal Attias, Andrea Kotzur, Richard and Latanya Bailey, and Lisa Huber; and as to all but Counts I and V for Connie and Curt Tringler."

3. **Related Cases**

The instant case was previously presented to this Court, styled United States Court of Appeals for the District of Columbia Circuit Case No. 16-7108. In that matter, this Honorable Court entered its opinion on August 1, 2017 reversing the trial court's August 10, 2016 order dismissing Plaintiffs' claims and remanded the matter for further proceedings.

[1] Citations to the joint appendix are referred to "(App. ___)."

TABLE OF CONTENTS

Page

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES i

TABLE OF AUTHORITIES v

STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION 1

STATEMENT OF THE ISSUES 1

STATUTES, RULES AND REGULATIONS 2

STATEMENT OF THE CASE 2

I. FACTUAL BACKGROUND 2

II. PROCEDURAL BACKGROUND 3

SUMMARY OF THE ARGUMENT 5

ARGUMENT 7

I. PLAINTIFFS' HAVE ADEQUATELY PLED ACTUAL DAMAGES. 7

A. Appellants' allegations adequately state actual damages. 7

1. *The district court's opinion is irreconcilable with this Court of Appeals' recent precedent in OPM Data Security Breach Litigation.* 11

2. *Failure to obtain a benefit-of-the-bargain is a legally cognizable actual damage.* 12

3. *The district court committed reversible error in finding no actionable breach of contract damages.* 14

B. Appellants' have plead legally cognizable actual damages in the form of non-economic loss from invasion of privacy. 19

C. The D.C. Plaintiffs' claim for statutory damages sufficiently states actual damages. 22

D. Appellants properly pled cognizable damages in their tort claims. 24

E. Appellants have stated legally cognizable damages in their claim for breach of the duty of confidentiality. 29

III. THE D.C. PLAINTIFFS HAVE ADEQUATELY PLED THEIR D.C. CPPA CLAIMS. 30

IV. THE COURT SHOULD RECOGNIZE AN INDEPENDENT DUTY TO SAFEGUARD SENSITIVE INFORMATION. 32

A. The Appellees routinely profit from taking individuals' private information and owes those individuals a duty to safeguard sensitive information. 32

B. The lower court misapplied *Choharis* 43

V. DISMISSAL OF PLAINTIFFS' UNJUST ENRICHMENT CLAIM WAS PREMATURE. 45

CONCLUSION 48

REQUEST FOR ORAL ARGUMENT 48

STATUTORY ADDENDUM

5 U.S. Code § 552a. Records maintained on individuals .....Add. 1

28 U.S. Code § 1291. Final decisions of district courts .....Add. 23

28 U.S. Code § 1332(d)(2) .....Add. 24

D.C. Code § 28-3905(k)(2) .....Add. 24

U.S. Constitution, Art. III .....Add. 25

UNPUBLISHED DECISION ADDENDUM
OPM Data Security Breach Litigation, Case No. 17-5217 (June 21, 2019)

RULE 32 CERTIFICATION

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Page(s)

Cases

Amnesty Int'l USA,
568 U.S. 398 (2013) 33

Anderson v. Hannaford Bros. Co.,
659 F.3d 151 (1st Cir. 2011) 33

**Attias v. Carefirst, Inc.*,
865 F.3d 620 (D.C. Cir. 2017),
cert. denied, 138 S. Ct. 981,
200 L. Ed. 2d 248 (2018)..... 4, 7, 8, 17, 18, 24, 25, 36

Austin-Spearman v. AARP & AARP Services Inc.,
119 F. Supp. 3d 1 (D.D.C. 2015) 16, 17

Bay General Industries, Inc. v. Johnson,
418 A.2d 1050 (D.C. 1980).....11

Beaven v. U.S. Dep't of Justice,
622 F.3d 540 (6th Cir. 2010).....28

Bell v. Michigan Council 25 of Am. Fed'n of State, Cty.,
Mun. Employees, AFL-CIO, Local 1023,
No. 246684, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005).....40

Brush v. Miami Beach Healthcare Grp. Ltd.,
238 F. Supp. 3d 1359 (S.D. Fla. 2017)..... 39, 40

Capital Keys, LLC v. Democratic Republic of Congo,
278 F.Supp.3d 265 (D.D.C. 2017) 13

Choharis v. State Farm Fire & Casualty,
961 A.2d 1080 (D.C. 2008)..... 6, 43, 44

Daly v. Metropolitan Life Insurance Co.,
782 N.Y.S.2d 530 (Sup.Ct.N.Y .Cty.2004).....41

---

*Authorities upon which we chiefly rely are marked with asterisks.

Dieffenbach v. Barnes & Noble, Inc.,
887 F.3d 826 (7th Cir. 2018) 7, 8, 9, 13, 33

District News Co. v. Goldberg,
107 A.2d 375 (D.C. 1954) 11, 19

District of Columbia v. Barriteau,
39 A.2d 563 (D.C. 1979) 20

Doe v. Chao,
540 U.S. 614, 124 S. Ct. 1204,
157 L. Ed. 2d 1122 (2004) 28

Doe v. Dominion Bank of Washington,
963 F.2d 1552 (1992) 37

Doe v. Medlantic Health Care Group, Inc.,
814 A.2d 939 (D.C. 2003) 21, 37

E. & M. Const. Co. v. Bob,
115 Ga. App. 127 (153 S.E.2d 641) 44

Fed. R. Civ. P. 12(b) 28, 29

Federal Aviation Admin. v. Cooper,
566 U.S. 284 (2012) ..... i, 11

Fero v. Excellus Health Plan, Inc.,
304 F. Supp. 3d 333 (W.D.N.Y. 2018) 33

Floyd v. Morgan,
106 Ga. App. 332 (127 S.E.2d 31) 44

Graham v. M & J Corp.,
424 A.2d 103 (D.C. 1980) 39

Hammonds v. Aetna Cas. & Sur. Co.,
7 Ohio Misc. 25 (N.D. Ohio 1965) 30

Haymon v. Wilkerson,
535 A.2d 880 (D.C. 1987) 20

Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.,
892 F.3d 613 (4th Cir. 2018) 33

In re Anthem, Inc. Data Breach Litig.,
2016 WL 3029783 (N.D. Cal. May 27, 2016) 33

In re Arby's Rest. Grp. Inc. Litig., No. 1:17-CV-0514-AT,
2018 WL 2128441 (N.D. Ga. Mar. 5, 2018) 33, 41

In re Experian Data Breach Litig., No. SACV 15-1592 AG (DFMx),
2016 WL 7973595 (C.D. Cal. 2016) 33

In re Sci. Applications Int'l Corp.,
45 F. Supp. 3d 14 (D.D.C. 2014) 16, 17

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) 33

In re Zappos.com,
888 F.3d 1020 (9th Cir. 2018) 8

In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.,
No. 1:14-MD-2583-TWT,
2016 WL 2897520 (N.D. Ga. May 18, 2016) 40

Jacobson v. Hofgard,
168 F. Supp. 3d 187 (D.D.C. 2016) 31

Jones v. Commerce Bancorp, Inc., No. 06 CIV. 835 (HB),
2006 WL 1409492 (S.D.N.Y. May 23, 2006) 41

Kline v. 1500 Massachusetts Ave. Apartment Corp.,
439 F.2d 477 (D.C. Cir. 1970)..... 37, 38

Kwikset Corp. v. Superior Court,
51 Cal. 4th 310,120 Cal. Rptr. 3d 741,
246 P.3d 877 (2011) 9

Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016) 33

Maxwell v. Gallagher,
709 A.2d 100 (D.C. 1998) 10

McKenzie v. Allconnect, Inc.,
369 F. Supp. 3d 810 (E.D. Ky. 2019) 41, 42

Moody v. Martin Motor Co.,
76 Ga. App. 456 (46 S.E.2d 197) 44

OPM Data Security Breach Litigation,
Case No. 17-5217 (June 21, 2019) 5, 7, 8, 11, 14, 17, 26, 27, 32, 33

Parr v. Ebrahimian,
70 F.Supp.3d 123 (D.D.C. 2014) 22, 23, 24

Pierce v. Underwood,
487 U.S. 552, 108 S.Ct. 2541,
101 L.Ed.2d 490 (1988) 11

Randolph v. ING Life Ins. & Annuity Co.,
973 A.2d 702 (D.C. 2009) 17, 18, 19, 20, 25, 26

Remijas v. Neiman Marcus Grp.,
794 F.3d 688 (7th Cir. 2015) 33, 35

Resnick v. AvMed, Inc.,
693 F.3d 1317 (11th Cir. 2012) 33, 39

Schiff v. Am. Ass'n of Retired Persons,
697 A.2d 1193 (D.C. 1997) 47

Shames-Yeakel v. Citizens Fin. Bank,
677 F. Supp. 2d 994 (N.D. Ill. 2009) 35

Slinski v. Bank of Am., N.A.,
981 F. Supp. 2d 19 (D.D.C. 2013) 31, 32

Smith v. Triad of Alabama, LLC,
2015 WL 5793318 (M.D. Ala. Sept. 29, 2015) 33

Stacy v. HRB Tax Grp., Inc.,
516 F. App'x 588 (6th Cir. 2013) 40

Suesbury v. Caceres,
840 A.2d 1285 (D.C. 2004) 30

Tate v. Aetna Cas. & Sur. Co.,
149 Ga. App. 123, 253 S.E.2d 775 (1979) 44

The Scowcroft Grp., Inc. v. Toreador Res. Corp.,
666 F. Supp. 2d 39 (D.D.C. 2009).....47

U.S. ex rel Landis v. Tailwind Sports Corp.,
234 F.Supp.3d 180 (D.D.C. 2017) 13

United House of Prayer for All People v. Therrien Waddell, Inc.,
112 A.3d 330 (D.C. 2015) 13

United States v. Bornstein,
423 U.S. 303, 96 S.Ct. 523, 46 L.Ed.2d 514 (1976) 13

Vassiliades v. Garfinckel's, Brooks Bros.,
492 A.2d 580 (D.C. 1985) 21, 30

Vector Realty Group v. 711 14TH STREET,
659 A.2d 230 (D.C. 1994) 13, 19

Workman v. United Methodist Comm. on Relief of Gen. Bd. of Glob. Ministries of United Methodist Church,
320 F.3d 259 (D.C. Cir. 2003).....38

Statutes

5 U.S.C. § 552a 27, 28

28 U.S.C. § 1291 1

28 U.S.C. § 1332(d)(2).....1

D.C. Code § 28-3905(k)(2)(A) 22, 23

D.C. Consumer Protection Procedures Act 30

U.S. Const., Art. III 14, 16, 19, 25, 26, 27, 36

Rules

Fed. R. Civ. P. 12 ..... 3, 16

Fed. R. Civ. P. 12(b)(6) 1, 16

Fed. R. Civ. P. 54(b) ..... ii, 5

Other Authorities

Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018 (in millions). Statista (last edited Feb. 26, 2019) (available at https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed) 34

D.C. Civ. Jur. Ins. § 11.31 12

D.C. Civ. Jur. Ins. § 20.11 23

Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber–Risk Insurance*, 3 J.L. & Cyber Warfare 1 (2014) 39

PROSSER & KEETON, *supra*, § 4 20

Restatement (Second) of Contracts § 347 11

RESTATEMENT (SECOND) OF CONTRACTS § 347 comment (1981) 13

RESTATEMENT (SECOND) OF TORTS § 901, comment (a) 20

STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

The United States District Court for the District of Columbia had jurisdiction under 28 U.S.C. § 1332(d)(2), and by virtue of the fact that all acts and omissions complained of occurred within the District of Columbia.

This Court's jurisdiction over the appeal from the district court's order granting Appellees' motion to dismiss rests on 28 U.S.C. § 1291.

The district court Order appealed from was entered on February 26, 2019, and the Appellants timely filed their Notice of Appeal, two days later, on February 28, 2019.

STATEMENT OF THE ISSUES

I. Whether data breach victims have unique pleading requirements as to damages.

II. Whether district court erred in granting Appellees' Motion to Dismiss Under Federal Rule of Civil Procedure 12(b)(6) on the grounds that Appellants have not sufficiently establish damages such that their case should be dismissed as a matter of law.

III. Whether the District of Columbia Consumer Protection Procedures Act is enforceable in the presence of a contract.

IV. Whether mitigation of damages is an actual damage in a breach of contract claim.

V. Whether a party may state an unjust enrichment case in the alternative to a contract claim in his complaint.

VI. Whether a company that acquires and profits from sensitive consumer information owes an independent duty to safeguard that information.

STATUTES, RULES AND REGULATIONS

The applicable statutes, rules and regulations are contained in the addendum to this brief.

STATEMENT OF THE CASE

I. FACTUAL BACKGROUND

In June of 2014, the sensitive and personal information of the Appellants,[2] along with more than one million other individuals, was obtained by data thieves who conducted a sophisticated cyberattack on Appellees'[3] servers. (App. 23, 119). CareFirst failed to recognize the attack had even occurred—given the apparent expertise of the attackers—until nearly a year after the breach. (App. 23-24, 119). On May 20, 2015, the members of the putative class were first notified that personal and sensitive information in the custody and care of CareFirst had been stolen. *Id*.

CareFirst admits that it was attacked and breached by a data thief and lost the information of more than a million people. (App. 24, 53-54). CareFirst offered to

---

[2] Chantal Attias, Andreas Kotzur, Richard and Latanya Bailey, Curt and Connie Tringler, and Lisa Huber (hereinafter "the Appellants" or "Plaintiffs") are the customers and insureds of CareFirst in the District of Columbia, Maryland and Virginia.

[3] CareFirst Inc., Group Hospitalization and Medical Services, Inc., CareFirst of Maryland, Inc., and CareFirst BlueChoice (hereinafter collectively referred to as "Appellees" or "CareFirst") is a network of for-profit health insurers which provide health insurance coverage to individuals in the District of Columbia, the State of Maryland and the Commonwealth of Virginia.

purchase identity theft protection—though not comprehensive—for the putative class. (App. 24). CareFirst even warned the victims about their need to seek identity theft protection. *Id*. Finally, CareFirst admitted that, at a minimum, the names, birthdays, email addresses, and subscriber identification numbers were stolen by the hackers. [4] (App. 53).

The Appellants each received a notification letter from CareFirst. After reviewing the letters and their options, the Appellants purchased more comprehensive identity theft protection to mitigate their harm, having determined that the risk of identity theft would not be adequately addressed by the protection offered by CareFirst. In addition, Curt and Connie Tringler suffered identity theft in the form of tax refund fraud. The parties ultimately joined in filing the Second Amended Complaint for damages.

II. PROCEDURAL BACKGROUND

This is the second appeal, regarding largely the same issues, where the Appellants are challenging a Rule 12 dismissal of their case. First, the district court concluded that the Appellants suffered no injury to confer standing. (App. 117, 119-

[4] The Appellants alleged that social security numbers were taken as well based upon the nature of the attack and expert opinion that data thieves do not leave always tracks without gaining such valuable information.

120). Now, the district court concluded that the Appellants suffered no damages. (App. 123-138).

The first challenge to the pleading occurred on September 24, 2015, when CareFirst filed its motion to dismiss for lack of subject matter jurisdiction and for failure to state claim. That motion was fully briefed, and on August 10, 2016, the district court entered a dismissal for lack of subject matter jurisdiction as to all Appellants on the basis that Plaintiffs-Appellants did not have standing to bring a claim. On September 6, 2016, the Appellants filed their appeal of the August 2016 dismissal to this Honorable Court. The issue was fully briefed, and oral argument was held. On August 1, 2017, this Circuit Court reversed the district court's dismissal, holding that the victims in this data breach do in fact have standing. *Attias v. Carefirst, Inc*., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981, 200 L. Ed. 2d 248 (2018) (*Attias I*).

On June 13, 2018 and upon remand to the district court, CareFirst renewed their motion to dismiss for failure to state a claim based on lack of damages. (App. 65). The renewed motion to dismiss for failure to state a claim was fully briefed and on January 30, 2019, the district court issued an order granting in part and denying in part the Appellees' motion. (App. 115, 116). The only individuals with any claims remaining following the district court's ruling were Curt and Connie Tringler's

whose claims for breach of contract and violation of the Maryland Consumer Protection Act survived. (App. 115).

On February 26, 2019, upon motion of its own and the parties, the district court entered final judgment pursuant to Federal Rule of Civil Procedure 54(b). (App. 158). This appeal of the second pleading dismissal was timely filed.

SUMMARY OF THE ARGUMENT

The district court committed reversible error by dismissing the majority of the Appellants' claims. Its basis for doing so was a misreading of this Court's reversal of its initial dismissal for lack of standing. The district court mistakenly relied on a case regarding standing (which this Court unequivocally ruled the Appellants had actually pled as concrete, particularized, and ***redressable***) to find that the Appellants had not pled damages sufficiently to survive a pleading-stage motion to dismiss.

The district court erred in its *second* pleading dismissal of this case with reasoning strikingly similar to the initial dismissal, which this Court reversed. The Appellants very clearly pled actual damages, both pecuniary and otherwise. The district court appears to misinterpret "actual damages," but this Court, very recently, in *OPM Data Security Breach Litigation*, Case No. 17-5217 (June 21, 2019) (slip opinion), analyzed several forms of damages that may take place in data breach cases involving cyber criminals. One of these forms, and the very least of the damages which the Appellants all pled in their Complaint, is simply time spent and lost in

addressing the theft of an individual's sensitive information. The Appellants also pled the cost of credit monitoring as a damage. The Appellants have undoubtedly pled real damages both in contract and tort, as well as statutorily.

Similarly, the district court misapplied this Court's ruling in *Choharis*, wrongfully broadening it to apply to any and all tort actions in which a contract exists, extending beyond the intended scope of first-party bad faith claims. The district court, despite other circuits' opinions recognizing a duty, denied any notion that an independent duty exists from businesses, which gather and profit from this data, to safeguard sensitive consumer information. Such a duty exists, and its existence is predicated on the well-established foreseeability that cyber criminals highly desire sensitive consumer information.

This case, despite being four years since inception, is still in the pleading stage, and is entirely without the benefit of discovery exchanged. The Appellants' well-pled complaint has suffered enough flawed scrutiny from an insurance company determined not to take responsibility for its allowance of over a million records to fall into criminal hands. The district court's dismissal of the Appellants' claims should be reversed, and this case finally allowed to proceed in a meaningful fashion.

ARGUMENT

I. PLAINTIFFS' HAVE ADEQUATELY PLED ACTUAL DAMAGES.

A. Appellants' allegations adequately state actual damages.

The district court stated it had accepted that Appellants had adequately pled "actual harm." However, the district court then determined that though redressable harm had occurred, damages had not been pled. *See District Court Opinion*, p. 8-9 (App. 124-125). ("The D.C. Circuit's standing ruling does not control whether plaintiffs have alleged actual harm for purposes of their state-law claims."). The district court's opinion, however, is inapposite with the law of the case, the recent Opinion of this Court, and is a "new label for an old error." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *In re OPM Data Security Breach Litigation*, Case No. 17-5217 (June 21, 2019) (slip opinion).

This Court reiterated its position that criminal hacker data breaches could be compensated through damages in *OPM Data Security Breach Litigation*, Case No. 17-5217 (June 21, 2019) (slip opinion). The *OPM* Opinion, in part relying on the reasoning in *Attias I*, stated as follows:

> Granting that it may well be impossible at this point to eliminate the risk of future identity theft stemming from the *OPM* breaches, the money damages Arnold Plaintiffs seek can redress certain proven injuries related to that risk (such as reasonably-incurred credit monitoring costs).

In re OPM Data Security Breach Litigation, Case No. 17-5217 (June 21, 2019) (slip opinion) (citing *In re Zappos.com*, 888 F.3d 1020, 1030 (9th Cir. 2018) ("The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages.") (citation omitted); *Attias*, 865 F.3d at 629 ("The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages.")). The Seventh Circuit also overturned dismissal by a district court for finding a failure to allege actual damages in the context of a data breach. *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018). The *Dieffenbach* Court was presented with allegations from two different plaintiffs suggesting the same types of damage alleged here: (1) lost time in restoring funds; (2) lost time "sorting things out;" (3) lost time in making purchases; and (4) loss of the benefit of her bargain; and 5) the cost of credit monitoring. *Id*. at 828-29, 829-30. The Seventh Circuit had no trouble finding damages were pled stating "Money out of pocket is a standard understanding of actual damages in contract law, antitrust law, the law of fraud and elsewhere. To get damages plaintiffs must show that a culpable data breach caused the monthly payments, but the complaint cannot be dismissed before giving the class an opportunity to do so." *Id*. at 830. The Court further ruled "there are innumerable ways in which economic injury—may be shown." *Id*. at 829

(quoting *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323, 120 Cal. Rptr. 3d 741, 246 P.3d 877 (2011). Further, the Court recognized that the "time value of money" validates a loss, as does "significant time and paperwork costs incurred to rectify violations." *Id*.

Appellants' economic and non-economic damages are each cognizable under the types of causes of action that were pled and fall into one of three categories: 1) contract claims; 2) tort claims; and 3) statutory claims. Each of these types of causes of action also specifically identify these losses as "actual damage." Accepting Appellants' allegations as true, they have pled actual damages in this case including both economic and non-economic damage. The allegations of actual damage include:

> 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.***
>
> 20. Many Plaintiffs and Class Members suffered from ***actual economic injury resulting in tax-refund fraud, identify theft, credit card fraud, and other conduct causing direct economic injury*** as a result of the identity theft they suffered when Defendants did not protect and secure their PII/PHI/Sensitive Information and disclosed their PII/PHI/Sensitive Information to hackers.
>
> 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.
>
> ***
>
> 37. Defendants suggested that Plaintiffs and each class member protect themselves with identity theft protection and monitoring to combat Defendants' failures to adequately and appropriately safeguard personal information, to identify a cyberattack in a timely fashion, and to provide the privacy security and safeguards promised in Defendants' Internet Privacy Policy.
>
> 38. Plaintiffs and members of The Class have suffered economic and non-economic loss in the form of mental and emotional pain and suffering and aguish as a result of Defendants' failures.

(App. 20-21, 24). (emphasis added). These allegations plainly allege two types of actual economic damage: 1) economic loss; and 2) non-economic loss in the form of emotional distress. Neither of these types of damage are novel theories of damage, nor are they controversial. Instead of accepting that "economic loss" and "non-economic loss" are well-established legal damages, the district court re-framed the allegations as "(1) actual and/or heightened risk of misuse of personal information, (2) loss of the 'benefit of the bargain' they struck when they purchased their policies, (3) consequential damages like expenditures credit monitoring services, and (4) emotional distress." (App. 127). The district court did not explain its definition of "actual damages," but actual damages are nothing more than "any loss" or "any compensable damage." *See Maxwell v. Gallagher*, 709 A.2d 100, 104 (D.C. 1998). The gravamen of "actual damage" is an allegation that a party suffered "any loss," and Appellants have alleged that as a consequence of Appellees' failures, breaches

and misrepresentations, they have suffered economic and non-economic damages, which are each the epitome of legal "actual damage." Decisions on "questions of law" are "reviewable de novo," while decisions on "questions of fact" are "reviewable for clear error." *Pierce v. Underwood*, 487 U.S. 552, 558, 108 S.Ct. 2541, 101 L.Ed.2d 490 (1988). The district court committed several reversible errors regarding questions of law. The Appellants adequately pled damages and the case should move forward beyond the pleading stage.

1. The district court's opinion is irreconcilable with this Court of Appeals' recent precedent in OPM Data Security Breach Litigation.

This Court recently issued its opinion in *OPM Data Security Breach Litigation*, Case No. 17-5217 (June 21, 2019) (slip opinion). *OPM* is dispositive of the issue of damages: "Incurred out-of-pocket expenses are the paradigmatic example of 'actual damages' resulting from the violation of privacy protections." *In re OPM* at *32 (citing *Federal Aviation Admin. v. Cooper*, 566 U.S. 284, 298 (2012)). This has always been the law in the District of Columbia, where a party may collect "an expense reasonably incurred" as a "proper element of consequential damages."[5] *District News Co. v. Goldberg*, 107 A.2d 375, 377 (D.C. 1954).

[5] *See also Bay General Industries, Inc. v. Johnson*, 418 A.2d 1050, 1057 n.19 (D.C. 1980); *see also Capital Keys, LLC*, 278 F.Supp.3d at 272-73 (quoting Restatement (Second) of Contracts § 347) ("Expectation damages typically are measured by (a) the loss in the value to [the injured party] of the other party's performance caused by its failure or deficiency, plus (b) any other loss, including incidental or consequential loss, caused by the breach, *less* (c) any cost or other loss that [the injured party] has avoided by not having to perform.")

Additionally, cognizable "Incidental damages include any costs [the plaintiff] incurred while making reasonable efforts to avoid losses, whether the efforts were successful or not." D.C. Civ. Jur. Ins. § 11.31. This is not novel; and the *OPM* Court merely reaffirmed these fundamentals in a data breach case. The Appellants sufficiently allege and seek mitigation costs. (App. 20). Therefore, ***all of the Appellants*** have actual damages in the form of mitigation costs as permitted in any District of Columbia contract matter.

OPM also found actual damages in the time spent "to resolve the fraudulent tax return filing and to close a fraudulently opened account. Those efforts 'required her to take time off work[]' to address the consequences of the *OPM* breach." ***All Appellants*** in this case plainly alleged they spent significant time to address this. *Id.* ("the Plaintiffs and Class Members have or will have to spend significant time and money to protect themselves…"). (App. 20). Therefore, all Appellants have pled actual damages. All Appellants' economic damages are cognizable and sufficient to state a claim for each of the Appellants and for each of the counts they pled: all contract, tort, and statutory causes of action.

2. Failure to obtain a benefit-of-the-bargain is a legally cognizable actual damage.

OPM is in accord with other Circuits which have reversed dismissal for an alleged lack of damages, but in addition to those damages at issues in *OPM*, other legally cognizable damages were pled. As stated *supra*, the Seventh Circuit recently

overturned dismissal by a district court for finding a failure to allege actual damages in the context of a data breach. *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018). A loss of the benefit-of-the-bargain is another tried-and-true allegation of actual damages. The damages sought in the Second Amended Complaint are the standard type of actual damages which District of Columbia law awards to a non-breaching party whose contract has been breached:

> 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.

Vector Realty Group v. 711 14TH STREET, 659 A.2d 230, 234 (D.C. 1994) (quoting RESTATEMENT (SECOND) OF CONTRACTS § 347 comment (1981)). "Under 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)). The benefit-of-the-bargain damage is the standard measure of damages in contract cases. *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.

Applying this benefit-of-the-bargain rule is straightforward in this matter. Appellants plainly alleged that:

> 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.

(App. 21). Therefore, Appellants have legally cognizable actual damages in the form of the loss of the benefit-of-the-bargain.

3. The district court committed reversible error in finding no actionable breach of contract damages.

For the reasons already stated, the district court's opinion is irreconcilable with *OPM* and immediate remand may be warranted in light of it. However, the district court's opinion was irreconcilable with well-established precedent even before *OPM*.

The district court mistakenly interposed the law of Article III standing onto the law of cognizable contract damages in a relentless attempt to advance a unique and novel body of law applicable only to data breach cases. Appellants only seek the

standard damages that are recoverable under controlling law. The district court found that Appellants' breach of contract action failed to state actual damages by ignoring this Court's law of the case, and misinterpreting case law from the District of Columbia Court of Appeals in an attempt to "achieve the same outcome it believes would result if the District's highest court considered this case." (App. 125). The district court was committed to finding (or creating) a separate body of law applicable only to data breach cases that defines actual damages at the motion to dismiss stage as something other than "the standard measure of actual damages." *Supra Capital Keys*, 278 F.Supp.3d at 272; *see also* Memorandum Opinion, (App. 129, 131) ("District of Columbia courts have not addressed whether a 'benefit-of-the-bargain' or 'overpayment' theory of damages is sufficient to state a claim for actual damages ***in the data-breach context***.") (emphasis added). But there is no basis to treat the Appellants' contract claim as anything other than a traditional contract claim for which the traditional measures of damages state a claim, and so its most obvious error was setting aside standard contract damages law in favor of creating a new law of "data breach damages" by applying legal principles of Article III standing requirements. Even assuming, *arguendo*, there is a unique definition of actual damages in data breach cases, Appellants have adequately pled those damages.

The district court discarded the benefit-of-the-bargain loss primarily by relying on two district court opinions which did not assess whether benefit-of-the bargain damages were "actual damages," but actually found that Article III standing was lacking. *See* Memo, pp. 14-15 (App. 128-129) (relying upon *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d 14 (D.D.C. 2014); *Austin-Spearman v. AARP & AARP Services Inc.*, 119 F. Supp. 3d 1 (D.D.C. 2015)). In *Austin-Spearman*, the district court found that because the plaintiff had "not plausibly claimed that she overpaid for the AARP membership agreement such that she was injured economically and now has standing to sue." *Id*. at 14. *In re SAIC* similarly found that the alleged loss of value did not support a finding of actual harm under the federal courts' standing analysis.[6] And the *SAIC* court specifically "reserve[d]the issue of whether Defendants' Rule 12(b)(6) Motions should be granted for a future date." *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d 14 at 34.

While the district court relied upon two standing decisions from other District of Columbia district courts, for some reason it did not credit this Court's most salient opinion on the point, which actually arose from this matter: *Attias v. Carefirst, Inc.*,

[6] The relevant facts of *SAIC* are starkly distinct from the instant matter and others in which *data thieves* accessed and stole data for its inherent value. As the *SAIC* court found, "the theft from the SAIC employee's car was a low-tech, garden-variety one. Any inference to the contrary is undermined by the snatching of the GPS and car stereo. This is hardly a black-ops caper." *In re SAIC.*, 45 F. Supp. at 33.

865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981, 200 L. Ed. 2d 248 (2018). In the instant matter, it is law of the case that the Appellants ***do have standing to sue*** which includes a binding ruling that Appellants have damages which are redressable.[7] Unlike *Austin-Spearman*, the *Attias* Appellants have plausibly claimed that they were harmed. From that harm, they have suffered and pled, legally cognizable contract damages, including, *inter alia*, loss of the benefit-of-the-bargain. If the district court had given this Circuit's *Attias* opinion the controlling impact it has, it would have found that the *Attias* plaintiffs have sufficiently pled actual damages and that they can "be made whole by monetary damages." *Attias*, 865 F.3d at 629. This point becomes even more apparent when considering this Court's recent ruling in *OPM*.

The district court reasoned around this Court's holding in *Attias* by noting that "standing and actual damages are separate questions…" and then, in the same breath, the district court relied on the district court opinions related to those very issues of standing, including *Austin-Spearman*, *SAIC*, and later *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702 (D.C. 2009). (App. 98-100, 125-126, 128-129, 132-133). (citing *Randolph*). But while the law of this Circuit is that the *Attias* Appellants have standing which can be redressed through monetary damages payments, all the

[7] The district court did not consider or analyze that *Austin-Spearman* and/or *In re SAIC* would have been decided differently, *even on the issue of standing*, with the benefit of *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

district court was required to do was apply traditional District of Columbia damages law when it, instead, **applied pre-*Attias* district court standing opinions**. This was plain error.

After ignoring the law of standing developed in *Attias* and applying pre-*Attias* district court standing opinion, the district court continued its error by misinterpreting the District of Columbia Court of Appeals opinion of *Randolph v. ING Life Ins. & Annuity Co*. *Supra*. In *Randolph*, the Court of Appeals made clear that it was dismissing the action for lack of subject matter jurisdiction, and not creating a body of "**data breach law of actual damages**." *Randolph* at 704 ("The Superior Court dismissed the suit for lack of standing. We affirm the order of dismissal.")(emphasis added).[8] Nevertheless, the district court relied on this standing opinion, in which a "home was burglarized [and] [a]mong the items stolen during the burglary was the agent's personal laptop computer, onto which he had downloaded, allegedly without encryption or password protection, personal information…" to hold that the Appellants, whose information was stolen under very different scenarios, and whom this Court already ruled has standing, including redressability, to suggest that the District of Columbia Court of Appeals created a

[8] *Randolph* did not include a claim for breach of contract at all. *Id*. at 705. Yet the district court extrapolated new law of contract damages from a case not involving a claim for breach of contract and decided on questions of standing.

per se rule that mitigation costs following any data breach are not contract damages. *Id*. at 704. This, again, is plain error.

The district court wrongly focused its analysis of damages on cases in which Article III standing was lacking. From opinions on standing, the district court wrongfully found a bright line rule that "time and money spent protecting against future identity theft cannot constitute damage…". This is inapposite with the District of Columbia's acceptance of consequential and incidental damages remedies in breach of contract actions. *Supra Vector Realty Group v. 711 14TH STREET*, 659 A.2d 230, 234 (D.C. 1994) (finding benefit-of-the-bargain damages are a standard measure of damages); *District News Co. v. Goldberg*, 107 A.2d 375, 377 (D.C. 1954) (finding mitigation costs are a measure of actual damages).

The district court engaged in reversible error in finding that there was no actionable damage in Appellants' contract claim.

B. Appellants' have plead legally cognizable actual damages in the form of non-economic loss from invasion of privacy.

Appellants' tort claims likewise seek those damages for which D.C. law permits recovery. These tort claims include Negligence, Negligence *Per Se*, Fraud, Constructive Fraud and Breach of the Duty of Confidentiality. Appellants have pled damages that are recoverable in tort:

> Plaintiffs and the Class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

(App. 34-35, 42-48). These damages, including a loss of their privacy and confidentiality rights, are standard damages sought in tort.

> The primary purpose of tort law is to compensate plaintiffs for injuries they have sustained due to the wrongful conduct of others. The normal measure of tort damages is the amount which compensates the plaintiff for all of the damages proximately caused by the defendant's negligence.

Haymon v. Wilkerson, 535 A.2d 880, 885 (D.C. 1987) (citing *District of Columbia v. Barriteau*, 39 A.2d 563, 566-67 (D.C. 1979); RESTATEMENT (SECOND) OF TORTS § 901, comment (a); PROSSER & KEETON, *supra*, § 4, at 20). Appellants' allegations are that they suffered injuries as a result of Appellees' negligence or other tortious activity, including economic and non-economic injury as identified. These are compensable actual damages in tort.[9]

Finally, Appellants are entitled to compensation for non-economic loss for their tort claims. "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

[9]The Court relies on the law of standing to claim that damages are lacking. (*See* App. 128) (citing *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 708 (D.C. 2009). The law of the case is that Appellants have standing at the pleading stage. The district court's ruling does not reasonably stand for the suggestion that actual damage has not been alleged because it relies upon the law of standing, not damages.

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.).

The relationship between insurance providers and patients, particularly when insurers acquire private medical information, is obviously a confidential one. To be actionable, a claim for breach of confidentiality in a medical context requires the "unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship." *Doe v. Medlantic Health Care Group, Inc.*, 814 A.2d 939, 950-51 (D.C. 2003) (citing *Vassiliades*, 492 A.2d at 591). The Appellants' information is certainly nonpublic and was known to CareFirst only by virtue of their confidential relationship with them; and at no point did any Appellant or class member consent to having such information disclosed to thieves who undoubtedly intended (and who still intend) to use it for nefarious purposes, nor was such disclosure to "hackers" a privileged one. Appellants' conduct resulted in the undeniable massive breach of confidential information and this claim should persist beyond the pleading stage.

As to this specific cause of action, all Appellants have legally sufficient damages for their non-economic loss.

C. The D.C. Plaintiffs' claim for statutory damages sufficiently states actual damages.

Appellants specifically draw the Court's attention to the D.C. CPPA claim made by Chantal Attias and Andrea Kotzur (hereinafter "the D.C. Plaintiffs"). In addition to the loss of actual time and money, the D.C. Plaintiffs seek statutory damages afforded to them by the D.C. CPPA. These legally sufficient damages defeat Appellant's motion as the D.C. Plaintiffs are not required to seek anything more to state a claim for damages, even assuming, *arguendo*, there is no sufficient allegation of "actual damages." Within their cause of action under the D.C. CPPA, "Mr. Kotzur and Mrs. Attias and members of the D.C. Class have been injured and seek the following for herself and on behalf of the general public and members of the class: (d) $1500 per violation or treble damages, whichever is greater." (App. 37). These statutory damages are expressly provided for by the D.C. CPPA. *See* D.C. Code § 28-3905(k)(2)(A).

Statutory damages are sufficient to defeat dismissal even in the absence of any other loss. In *Parr v. Ebrahimian*, 70 F.Supp.3d 123 (D.D.C. 2014) (Friedman, J.), defendants moved for *summary judgment after extensive discovery*, and alleged that the plaintiff had failed to provide evidence of damages that would entitle her to relief under the D.C. CPPA. The defendants in that case argued that "even with the benefit of discovery, Ms. Parr has failed to produce evidence sufficient to support a reasonable jury's finding that any misrepresentations regarding code compliance

caused her any damages." *Id*. at 135. The *Parr* court correctly held "The CPPA also provides for recovery where a violation of its provisions does not cause actual harm to the consumer; in such cases, the consumer may be able to collect statutory damages in the amount of $1500 per violation." *Id*. (citing D.C. Code § 28–3905(k)(2)(A). Then, the district court definitively found "The Court concludes that Ms. Parr has raised genuine issues of fact regarding whether Rimcor's representations ***regarding code compliance*** and housing inspections could constitute a violation of one or more of the CPPA provisions cited *supra*, ***which could entitle her to recover statutory damages***." *Id*. (emphasis added).[10] Ms. Parr was entitled to trial by jury, defeating summary judgment without evidence of actual damages, based upon the available statutory damages. *See also* D.C. Civ. Jur. Ins. § 20.11, Liability Without Proof of Actual Harm ("It is conceivable a plaintiff could bring a CPPA action seeking the minimum statutory damages of $1,500 and injunctive relief without pleading or proving any actual damages.").

The D.C. Plaintiffs have brought a claim under the D.C. CPPA claim seeking, *inter alia*, statutory damages. Even assuming *arguendo*, that they have failed to

[10] The district court additionally found evidence of separate and distinct, but "probably minimal," damages were available under the D.C. CPPA. But specifically, as to housing "code compliance," the district court found no actual loss occurred, yet she was still entitled to a trial by jury on the question of statutory damages.

allege actual damages, the D.C. Plaintiffs' claim for statutory damages sufficiently states actual damages on its own.[11]

D. Appellants properly pled cognizable damages in their tort claims.

The district court in this case dismissed all of the Appellants' tort claims based on its misinterpretation that the Appellants did not plead actual damages in their pleading. First, it is important to note that this line of reasoning for finding dismissal appropriate at the pleading stage is suspiciously similar to the district court's finding that the Appellants lacked standing for want of an adequately pled injury-in-fact. *See* First District Court Dismissal (App. 52). This Court reversed the district court's first pleading dismissal on the grounds that a cognizable injury was pled, stating unequivocally that "identity theft…constitute[s] a concrete and particularized injury," *Id.* at 627.[12] but now, the same district court claims the cognizable injuries which the Appellants undoubtedly alleged do not qualify as "actual damages." The district court finds itself in the precarious position of standing for one of the alternative notions that either a) this Court's finding that concrete, particularized injuries-in-fact were alleged by the Appellants sufficient to meet the low bar

[11] There is no argument that the D.C. Plaintiffs' claim does not allege material and/or misleading statements that suffice as violations of the D.C. CPPA. *See id*. at 135, 136.

[12] This Court's ruling can rightfully be read as standing for the position that the *theft* of sensitive information by criminals, even absent the immediate *use* of one's identity, is a cognizable injury.

requirement of Article III standing was not to be followed; or b) sufficiently pleading concrete, particularized injuries-in-fact somehow is not sufficient to overcome dismissal for want of pled damages at the pleading stage.

The district court overlooks portions of this Court's reversal of its initial dismissal of this case that mentioned damages. This Court, in *Attias*, stated:

> Clapper recognized that where there is "a 'substantial risk' that a harm will occur, [this risk] may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," and a court can award damages to recoup those costs. *See* 568 U.S. at 414 n.5. **Plaintiffs allege that they have incurred such costs**: "the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, [the] cost of conducting a damage assessment, [and] mitigation costs." J.A. 5-6. To be sure, such self-imposed risk-mitigation costs, when "incurred in response to a speculative threat," do not fulfill the injury-in-fact requirement. *Clapper*, 568 U.S. at 416-17. But they can satisfy the redressability requirement, when combined with a risk of future harm that is substantial enough to qualify as an injury in fact. **The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages.**

Id. (emphasis added).

Again, it is especially confounding how the district court chose to rely upon *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702 (D.C. 2009) to defiantly state that "the District of Columbia Court of Appeals has expressly declined to treat an increased risk of future identity theft as an actual harm for purposes of negligence and breach of fiduciary duty claims based on data breaches." (App. 128, 133). The district court disregards the Appellants' proper argument that *Randolph* was a case

deciding standing, and focuses on this Court's approach in that case of analyzing the complaint for its success in stating a claim. *Id.* The district court's focus here is misplaced, and, again, completely dismisses this Court's ruling overturning its initial dismissal for standing. The complaint and claims brought in *Randolph*, and the harms alleged, are similar (even if less concrete and particularized) to the instant case, in which this Court declined to perform such an analysis in favor of unequivocally finding that the Appellants have alleged such injury sufficient for Article III standing.

The difference in approach between these two (2) cases obviously puts them at odds, with *Randolph* finding the plaintiffs lacked Article III standing, and this Court in *Attias* finding otherwise. If the district court truly felt bound by the decade-old case seemingly at odds with the very case which this Court had remanded to it, then it should have logically extrapolated that, if an analysis in *Randolph* that actual damages were not sufficiently pled led to a finding that the plaintiffs lacked standing, then, by finding that the Appellants in this case *did* have standing to bring suit, any analysis regarding actual damages was unnecessary and would have led to a finding that such were sufficiently pled.

This Court recently addressed the issue of damages in data breach cases. In *OPM*, decided June 21, 2019, a data breach occurred which affected more than twenty-one million people. *OPM*, at 3. While the plaintiffs in that case pled that

some had suffered unauthorized charges to their credit accounts and misuse of their social security numbers, others had "yet to experience a fraud incident" but had spent time and money monitoring against identity theft. *OPM*, at 8. In an extremely similar circumstance, the district court in *OPM* dismissed the majority of the plaintiffs' claims, finding that only those who had already suffered an out-of-pocket loss had an injury-in-fact sufficient to pass Article III scrutiny, but even those which lacked standing for want of their injuries being "fairly traceable" to *OPM's* data breach. *OPM*, at 10. This recently reversed analysis strikes the very same chord as the district court in the instant appeal.

While this Court's analysis of damages in *OPM* was in the context of a violation of the Privacy Act, 5 U.S.C. § 552a, the analysis specifically regards "actual damages" at the pleading stage of a data breach litigation. *OPM*, at 31-38. Similar to the district court's ruling in this case, the district court in *OPM* found that only two of the potentially millions of putative class members had sufficiently plead actual damages. This Court disagreed, finding that other class members' injuries were sufficient to constitute actual damages. A focus of the analysis was the district court's reading of the plaintiffs' complaint in *OPM* allowing inferences in favor of the *defendant*. *Id.* Notably for the instant case, this Court recognized in *OPM* a plaintiff's time concentrated and lost to the monitoring and security of his or her identity undoubtedly qualifies as an actual damage. *Id.* at 35 (citing *Beaven v. U.S.*

Dep't of Justice, 622 F.3d 540, 557 (6th Cir. 2010) (plaintiffs can claim damages for "lost time" spent "dealing with the disclosure" of their personnel files).[13]

This Court's analysis of *OPM* through the lens of the Privacy Act is important because, even under that Act which requires proven pecuniary and economic harm, it is clear that the Appellant's tort claims survive a 12(b) motion to dismiss. However, while the district court and its authority for dismissal would seem to equate these terms inextricably with out-of-pocket damages, the Supreme Court of the United States has declined to do just that. In fn. 12 of *Doe v. Chao*, 540 U.S. 614, 627, 124 S. Ct. 1204, 1212, 157 L. Ed. 2d 1122 (2004), the Court states in regard to the Privacy Act's requirement of actual damages that it "[does] not suggest that out-of-pocket expenses are necessary for recovery of the $1,000 minimum; only that they suffice to qualify under any view of actual damages." *Id.*

The Appellants' pleading in the instant case inarguably pleads actual damages for each of its tort claims, the *very least of which* is the time the Appellants must spend monitoring their credit when they otherwise would not have had to. *See*, Pls. Cmplt., ¶¶ 16, 51, 83, 110, 117, 124. (App. 20, 26, 35, 41-43).

[13] Again, while *Beaven* was decided in the context of the Privacy Act, 5. U.S.C. § 552a, its analysis of what qualifies as "actual damages" is applicable to the instant case.

It is important to emphasize that, although it has been litigated for several years now, **this case can rightfully be categorized as in its infancy**. No discovery has been exchanged and no meaningful litigation progress has been made. It has never been held that an injured party must prove every element of every claim she brings against a defendant at the pleading stage. On the issue of damages, the Appellants have properly alleged actual damages – as noted by this Court in finding that the Appellants have properly alleged concrete, particularized injury – sufficient to overcome a 12(b) motion to dismiss. The Appellants – the injured parties – still have not had the benefit of discovery from the Appellees that lost millions of their records. Regardless, they have alleged real damages which are provable, and therefore, the district court's dismissal of the Appellants' tort claims should be reversed by this Court.

E. Appellants have stated legally cognizable damages in their claim for breach of the duty of confidentiality.

Appellees do not dispute that they breached the sensitive and legally protected medical information of more than a million people. Instead, Appellees argue they owe no duty to preserve and protect confidentiality. The duty of confidentiality exists not only by virtue of the contractual relationship, but also inherently according to the very sensitive nature of the personal information which was to be safeguarded in this case. The right to privacy and duty of secrecy should be analyzed against the backdrop of public policy, and, when repugnant to such, is subject to a valid cause

of action. *See Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580, 590 (D.C. 1985.[14] *See also Suesbury v. Caceres*, 840 A.2d 1285, 1287 (D.C. 2004); *Hammonds v. Aetna Cas. & Sur. Co.*, 7 Ohio Misc. 25 (N.D. Ohio 1965). Again, at the pleading stage, the Appellant's allegations are sufficient.

III. THE D.C. PLAINTIFFS HAVE ADEQUATELY PLED THEIR D.C. CPPA CLAIMS.

Chantal Attias and Andrea Kotzur (hereinafter "the D.C. Plaintiffs") brought a claim individually and on behalf of the relevant classes for violation of the D.C. Consumer Protection Procedures Act (hereinafter "CPPA"). (App. 35-36). The district court dismissed the claim by finding that the D.C. Plaintiffs' D.C. CPPA claim was either 1) premised on the contract; or 2) an "intentional breach of contract" and that D.C. law barred a CPPA claim in both instances. (App. 154-155). The district court's finding fails on the allegations and on the law.

The D.C. Plaintiffs' allegations of fact related to the D.C. CPPA claim make absolutely zero mention to the terms of the contract. (App. 35-37). The allegations reference an Internet Privacy Policy, not a contract. This policy is clearly pled to be outside the contract. There is absolutely no allegation that a breached term of the

[14] "In other jurisdictions, in the absence of legislation, courts have found the basis for a right of action for breach of the physician-patient confidential relationship in four main sources of public policy: state physician licensing statutes, evidentiary rules and privileged communication statutes which prohibit a physician from testifying in judicial proceedings, common law principles of trust, and the Hippocratic oath and principles of medical ethics."

contract, intentional or intentionally breached, is in any way part of the D.C. CPPA claim.

Additionally, the district court made great leaps in the law to dismiss this claim. *Jacobson v. Hofgard*, 168 F. Supp. 3d 187 (D.D.C. 2016) expressly rejected the insinuation that a plaintiff may not have both a breach of contract and a D.C. CPPA claim.

> Defendants contend that Plaintiffs have failed to state a claim because their District of Columbia Consumer Protection Procedures Act ("CPPA") claim "is barred by its equivalence to their breach of contract claim."…In other words, Defendants urge dismissal of the CPPA for the same reasons as the fraudulent misrepresentation claim. For the same reasons that the court rejected Defendants' arguments for dismissal of Plaintiffs' fraudulent misrepresentation claim, it rejects Defendants' arguments for dismissal of Plaintiffs' CPPA claim.

Jacobson v. Hofgard, 168 F. Supp. 3d 187, 207 (D.D.C. 2016). To the extent Jacobson "implied that a D.C. CPPA claim must be premised on at least *some* additional conduct other than a run-of-the-mill breach…" the D.C. Plaintiffs pled the existence of an Internet Privacy Policy outside the contract that made false and misleading representations.

Relatedly, the district court interpreted the D.C. Plaintiffs' CPPA claim, which makes no reference to any contract, as alleging an "intentional breach of contract." Memo. p. 39 (App. 154). The district court relied in *Slinski v. Bank of Am., N.A.*, 981 F. Supp. 2d 19 (D.D.C. 2013) to determine this is impermissible. But *Slinksi* similarly involved a claim in which there was no alleged misrepresentation

outside the four corners of the contract. "The only false misrepresentation that the plaintiffs identify is Freddie Mac's signing of the contract of sale which, they say, represented an intention to sell the condominium to Ms. Slinski, when in fact Freddie Mac always intended to sell it to Bank of America." *Slinski v. Bank of Am., N.A.*, 981 F. Supp. 2d 19, 32 (D.D.C. 2013). *Slinski* is facially distinct on its factual allegations. And there is no law in the District of Columbia that the mere presence of a breach of contract defeats a D.C. CPPA claim based upon extra-contractual misrepresentations.

IV. THE COURT SHOULD RECOGNIZE AN INDEPENDENT DUTY TO SAFEGUARD SENSITIVE INFORMATION.

A. The Appellees routinely profit from taking individuals' private information and owes those individuals a duty to safeguard sensitive information.

Companies have a legal duty to use reasonable efforts to protect confidential consumer information from foreseeable harm such as the risk of a criminal data breach. While not unanimous, there is an emerging judicial consensus that private companies acquiring sensitive information from individual's owe a duty to safeguard that information.

There is a substantial body of case law across the country, including this Court's ruling in *OPM*, establishing that criminal data breach victims whose personal information is stolen have suffered a legally cognizable injury and may recover for their time, effort and money spent redressing identity theft and fraud that

has occurred. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323-24 (11th Cir. 2012); *Arby's*, 2018 WL 2128441, at *11 n.12; *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 165-67 (1st Cir. 2011); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622, 623 n.9 (4th Cir. 2018); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016); *Remijas*, 794 F.3d at 692-94; *Smith v. Triad of Alabama*, LLC, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *14-16 (N.D. Cal. Aug. 30, 2017); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *14-15 (N.D. Cal. May 27, 2016); *Experian*, 2016 WL 7973595, at *5; *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 345 (W.D.N.Y. 2018). This is in addition to significant law, again including this Court's ruling in *OPM*, reasoning that mitigation of substantial risk of future harm, such as by purchasing credit monitoring services, is a legally cognizable injury. *Anderson*, 659 F.3d at 165-66; *Hutton*, 892 F.3d at 622; *Remijas*, 794 F.3d at 692-94; *Yahoo*!, 2017 WL 3727318, at *16; *Anthem*, 2016 WL 3029783, at *16; *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013); *In re OPM Data Security Breach Litigation*, Case No. 17-5217 (June 21, 2019) (slip opinion).

The point is that victims of criminal data breaches are routinely permitted to pursue negligence claims against companies that do not use reasonable cybersecurity measures to protect consumers' confidential information, which Appellants alleged.

Businesses like the Appellees trade on individuals' information. An individual's identifying information – the practical totality of which must be submitted to the Appellees in order to become its customer – as well as his or her health care documentation and payment data are not merely necessary elements of the Appellees' ability to provide its service and thereby garner revenue; such information is the Appellees' stock-and-trade.

There is an obvious reason why the Appellees are able to profit from their individual consumers' personal information – **that information has value**. And just as the information has value to the Appellees, so does it have value to others ***because consumers' personal information is intrinsically valuable***. This concept requires little explanation: There were more than twelve hundred (1,200) data breaches exposing nearly four and a half billion (4,500,000,000) patient or consumer records in 2018, alone.[15]

[15] Statista Research Dept. *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018* (in millions). Statista (last edited Feb. 26, 2019)(available at https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed).

Thieves do not steal that which is worthless. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015).[16] As an analogy, a consumer, in order to patronize the services of a bank, entrusts that bank with his or her wealth on the assurance – implied or explicit – that the bank has invested in and maintained practices and procedures which ensure that the customer's money is protected. A bank that failed to do so would find it difficult indeed to convince its customers or, to be sure, any court, that it had no duty to safeguard that with which it was entrusted and the very thing around which its business model is centered.[17]

There is, indeed, no discernible difference between a bank which transacts in (increasingly virtual, data-represented) money and a business such as CareFirst, which relies on the inherently valuable personal, sensitive information of its customers in order to be profitable. The enriching benefit bestowed upon CareFirst

[16] "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

[17] It is telling that a bank typically would not make this argument to begin with, as any bank that claimed it did not owe its customers a duty to protect their accounts would assuredly lose those customers. *See Shames-Yeakel v. Citizens Fin. Bank*, 677 F. Supp. 2d 994, 1008 (N.D. Ill. 2009) ("Citizens does not dispute that it had a duty to protect Plaintiffs' account from fraudulent access, but it does contest whether Plaintiffs have produced sufficient evidence of breach or causation."). It is alarming that healthcare insurance providers like CareFirst operate under such a lack of regulation and competition that these concerns are not shared.

and every other business which is dependent upon consumers' personal data for revenue naturally imparts a responsibility to safeguard that data. It cannot be otherwise. By collecting a consumer's personal, sensitive information and storing it for later, advantageous use, the Appellees have created a duty to safeguard that lucrative data, a breach of which is actionable in the courts of this country. Such actions are beneficial to the free market, as malfeasance is remedied economically, acting as both a deterrent against negligence, as well as a boon to competition to do better. Refusal to provide any redressability for victims of data breaches only perpetuates the appalling rate at which individuals' information is hijacked.

This Court, having heard this case before on the issue of Article III standing, found that, allowing for every inference in the Appellants' favor, that the Appellants did have standing because they suffered an actual, concrete injury. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 627, *cert. denied*, (D.C. Cir. 2017). Working backward from the Court's reasoning, if an injury-in-fact has been sufficiently alleged under a theory of negligence, then such injury must have a cause – the breach of a duty owed. That duty can only be the safeguarding of sensitive information (hence the commonplace nominative descriptor "data breach"). This Court found that, for purposes of Article III standing, the Appellants' pleading sufficiently pled injury that is "fairly traceable" to the Appellees. *Id.* at 629 ("Because we assume, for purposes of the standing analysis, that plaintiffs will prevail on the merits of their claim that

CareFirst failed to properly secure their data and thereby subjected them to a substantial risk of identity theft [citation omitted](emphasis added), we have little difficulty concluding that their injury in fact is fairly traceable to CareFirst."). This Court's own language regarding standing gives the impression that it understands the Appellant's allegations to be owing to CareFirst's breach of its duty to safeguard their information, and, therefore, such a duty must independently exist.

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 reasoned that a landlord had a duty to protect customers of a retail building because the 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. This Court, in another landlord-tenant case, *Kline v. 1500 Massachusetts Ave. Apartment Corp.*, 439 F.2d 477, 482-83 (D.C. Cir. 1970), went on to state:

> Other relationships in which similar duties have been imposed include landowner-invitee, **businessman-patron**, employer-employee, school district-pupil, hospital-patient, and carrier-passenger. In all, the theory of liability is essentially the same; that **since the ability of one of the parties to provide for his own protection has been limited in some way by his submission to the control of the other, a duty should be imposed upon the one possessing control (and thus the power to act) to take reasonable precautions to protect the other one from**

> **assaults by third parties which, at least, could reasonably have been anticipated**. However, there is no liability normally imposed upon the one having the power to act if the violence is sudden and unexpected provided that the source of the violence is not an employee of the one in control.

Id. (emphasis added).

The Court's reasoning in these cases was prescient in the realm of cybercrime and data breaches, and is especially apt to this case. When becoming a consumer of a healthcare insurance provider such as the Appellees, a person turns over to the CareFirst nearly every portion of identifying, sensitive information about herself, including biographical, medical, and financial data. Once submitted, the consumer has no method of monitoring the healthcare insurance provider's use of its data, nor does she have any control over the company's security monitors and measures. It is apparent that, as consumers required to entrust to the Defendant myriad sensitive data, the Appellants had a special relationship with Appellees and were owed a duty from the CareFirst to safeguard their sensitive information.

Interestingly, when deciding the existence of a duty, 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. *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 inappropriate.

Several of this Court's sister circuits have determined an independent duty to safeguard consumer information exists. The Eleventh Circuit has found this to be unreserved. In *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017), the court reiterated the position that:

> It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information:
>
> Financial institutions and health care providers possess a very high duty to protect consumer data residing on their networks and therefore a serious potential level of loss exposure. Firms that collect and retain such statutorily protected data must comply with internal controls and reporting standards set by the state and federal government. Even entities that are not specifically covered by laws or regulations pertaining to their specific industry are charged with a general duty to safeguard the consumer data under their control.

Id. (quoting Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber–Risk Insurance*, 3 J.L. & Cyber Warfare 1, 11 (2014)).

That court went on to cite as authority that an independent duty to safeguard private data exists in the Eleventh Circuit case of *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012), which found, "implicitly, that healthcare providers owe

patients a duty to protect their sensitive data." *Brush v. Miami Beach Healthcare Grp. Ltd.*, 283 F. Supp. 3d, at 1365. *See also In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016).[18]

The Sixth Circuit, as well, has recognized this duty to exist and be established by the relationship of the parties. *See Stacy v. HRB Tax Grp., Inc.*, 516 F. App'x 588, 591 (6th Cir. 2013). In *Stacy*, the Sixth Circuit stated that:

> [U]nder certain circumstances, a special relationship can exist between a defendant and plaintiffs such that the defendant does owe the plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information, information which easily could be used to appropriate a person's identity.

Id. (citing *Bell v. Michigan Council 25 of Am. Fed'n of State, Cty., Mun. Employees, AFL-CIO, Local 1023*, No. 246684, 2005 WL 356306, at *5 (Mich. Ct. App. Feb. 15, 2005).

[18] "The Court declines the Defendant's invitation to hold that it had no legal duty to safeguard information even though it had warnings that its data security was inadequate and failed to heed them**. To hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyberattacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk.** The Defendant's motion to dismiss based on the economic loss rule should be denied. Additionally, the Defendant moves to dismiss the Plaintiffs' negligence claim on the ground that it owed no duty to the Plaintiffs. **Because this Court finds that a duty does exist**, the motion to dismiss on the ground that there was no duty should also be denied." *Id.* (emphasis added).

District courts, as well, have considered this issue. In *Jones v. Commerce Bancorp, Inc.*, No. 06 CIV. 835 (HB), 2006 WL 1409492, at *2 (S.D.N.Y. May 23, 2006), the Southern District Court of New York held that a duty to safeguard consumer information arises when patronage is contingent upon the provision of a consumer's personal, sensitive information. *Id.* (citing *Daly v. Metropolitan Life Insurance Co.*, 782 N.Y.S.2d 530, 532 (Sup.Ct.N.Y .Cty.2004)).[19] Similarly cited and then rejected by the district court in this case under faulty premises based upon fiduciary duty which was not discussed in the underlying case, the district court for the Northern District of Georgia, in *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *7 (N.D. Ga. Mar. 5, 2018), very clearly found there to be a duty to protect personal credit card data of consumers from third party hacking in a business/consumer relationship. *Id.* In *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019), the district court for the Eastern District of Kentucky analyzed an employer's duty to safeguard employee information when the provision of such information was made a condition of employment and stated:

> …[w]hile Allconnect may not have had a duty to protect its employees from unknown or unforeseen third-parties, Allconnect did have a duty

[19] The district court in this case distinguished this opinion and its authority based upon the contention that, in this Circuit, the insurer-insured relationship is not a fiduciary one. However, the portion of the *Jones* opinion cited does not deal with breach of a fiduciary relationship, but solely with negligence. *Id.* The district court for the S.D.N.Y. addressed the fiduciary relationship separately. *See id.* at *3. The district court erred in its reasoning for distinguishing this case in favor of district opinions with no more precedential value.

> to prevent foreseeable harm to its employees and, as part of that duty, **had a duty to safeguard the sensitive personal information of its employees from unauthorized release or theft**. Of course, that is not to say that the Plaintiffs have demonstrated that the duty was breached in this case but only that, when reading the complaint in the light most favorable to the Plaintiff and assuming the facts as true, that the Plaintiffs have pleaded sufficient factual information in their complaint to demonstrate they were owed a duty of care.

Id. (emphasis added).

Data breaches will not abate from the criminals' end. Never will consumer information – especially sensitive identifying, medical, or financial data – be safe from enterprising thieves desire to take it. It is simply too valuable and, currently, woefully easy to purloin. The *primary and only* entities in a position to protect this sensitive data are those who collect it, compile it, and utilize it for profit. Unfortunately, these entities which maintain such databases *to make money* are the targets of cybercrime and have done little to protect against it. CareFirst and companies like it should never be able to deny their duty to safeguard their revenue-producing information. It cannot be stressed enough that the recognition of a duty to safeguard consumer information cannot be claimed an undue burden to businesses that make money off that very information. That is the trade-off. A business profits from its customers' information; that business must also protect it, or be held accountable for its negligence in tort.

B. The lower court misapplied *Choharis*

The district court erroneously held that *Choharis v. State Farm Fire & Casualty*, 961 A.2d 1080 (D.C. 2008) precludes *any and all* tort actions when a contract exits. (App. 140-143, 151). However, *Choharis* adopts a much narrower view that the District of Columbia does not have a first-party bad faith cause of action.

> Choharis principally challenges the refusal to recognize a tort of bad faith by insurance companies in the handling of policy claims. He asserts that a number of jurisdictions have recognized such a tort and that the District of Columbia should do the same. Although a common-law court, we are not persuaded that we should do so.

Id. at 1087. Instead of standing for the more expansive ruling that any tort claim may not arise out of a contractual relationship, *Choharis* limits its findings to the mere proposition that there is no first-party bad faith action in the District of Columbia for an insurer's failure to provide covered insurance claims. In fact, *Choharis* clearly indicated that the Court was not excluding tort claims against insurers:

> 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 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.

Id. at 1088. As indicated by this, *Choharis* merely held that a claim for a failure to provide the insurance benefits contracted for is addressed via contract law and not a newly created special tort of first-party bad faith.

The district court misinterpreted the application of *Choharis* with regards to the claims of fraud and negligent misrepresentation. (App. 141-142). In making its ruling, the district court ignored that tort claims could exist independent from a contractual relationship. The *Choharis* court specifically notes, "[a]lthough we reject the broad claim of bad faith as a viable tort, a cause of action that could be considered a tort independent of contract performance is a viable claim, even in the insurance context." *Choharis* at 1089-90. As such, the district court has plainly misinterpreted the scope of the holding in *Choharis*.

Furthermore, Appellants have made no claim that CareFirst, *et al*. failed to provide the *insurance benefits* that were bargained for, and have no such pleading of a first-party bad faith claim. Instead, Appellants complain of an "independent injury over and above the mere disappointment of plaintiff's hope to receive his contracted-for benefit." *Id*. at 1089; see also *Tate v. Aetna Cas. & Sur. Co.*, 149 Ga. App. 123, 124-25, 253 S.E.2d 775, 777 (1979) (*citing E. & M. Const. Co. v. Bob*, 115 Ga. App. 127 (153 S.E.2d 641); *Floyd v. Morgan*, 106 Ga. App. 332 (127 S.E.2d 31); *Moody v. Martin Motor Co.*, 76 Ga. App. 456 (46 S.E.2d 197) ("It is well settled that misfeasance in the performance of a contractual duty may give rise to a tort

action."). Appellants' Second Amended Complaint makes absolutely no allegation as to the denial of health insurance benefits. Rather, Appellants explicitly complain of Appellees' negligent security policies and unlawful trade practices that caused a loss of sensitive information. This negligent act caused an independent harm that gives rise to tort cause of action under D.C. substantive law.

V. DISMISSAL OF PLAINTIFFS' UNJUST ENRICHMENT CLAIM WAS PREMATURE.

The lower court prematurely dismissed the Appellants' unjust enrichment claim finding that a contractual relationship among the parties precluded a claim for unjust enrichment. (App. 152-153). The court's finding of a contractual relationship was based on Appellees' representations *during the dispositive motion hearing*, was the basis for dismissing the unjust enrichment claim. (App. 86-88). This dismissal is unwarranted because Appellants pled in the alternative three separate theories at this early stage of the proceedings because plaintiffs are entitled to plead alternative theories of relief. Obviously, the Appellants did not have the benefit of Appellees' admission during a hearing at the time the pleading was drafted. The district court effectively ruled that representations of defendant's lawyers during hearings could be relied upon to dismiss claims. Again, at the time the pleading was drafted, the Appellants did not have the benefit of Appellee's lawyer's admission that an express, valid, and enforceable contract existed. Instead, the Appellants properly pled

alternative theories of relief including breach of express contract, implied contract, and unjust enrichment.

Because it was unknown if express valid contracts existed that covered the protection of sensitive information, the Appellants properly alleged in the alternative as follows: “To the extent that it was not expressed, an implied contract was created whereby Defendants’ promised to safeguard Appellants’ health information and Sensitive Information from being accessed, copied, and transferred by third parties.” (paragraph 70 of complaint) (App. 33). It is clear from this allegation that the Appellants’ are not certain of the existence of valid enforceable express contracts and chose to allege in the alternative. The Appellants properly alleged in the alternative that the Appellees breached an express contract, or if no express contract existed, breached an implied contract, or if no implied contract governed the relationship, that Appellees were unjustly enriched. This is proper because:

> Under District of Columbia law, “there can be no claim for unjust enrichment when an express contract exists between the parties." Under the Federal Rules of Civil Procedure, however, a plaintiff may plead alternative theories of recovery. Courts in this District have found that a plaintiff should be permitted to plead both breach of contract and unjust enrichment. Such a conclusion is in the interest of justice -- to find that a plaintiff may not plead unjust enrichment where he or she also has alleged a breach of contract could leave that plaintiff without any remedy should the fact-finder determine at a later stage that there was no express agreement between the parties.

The Scowcroft Grp., Inc. v. Toreador Res. Corp., 666 F. Supp. 2d 39, 44 (D.D.C. 2009) (quoting *Schiff v. Am. Ass'n of Retired Persons*, 697 A.2d 1193, 1194 (D.C. 1997).

The district court's finding that the allegations must include specific language that the express contract is invalid or unenforceable misses the point that the allegations already alternatively plead "To the extent that it was not expressed..." regarding the very existence of a contract. (App. 33). In the instant case, Appellants have alleged by implication the invalidity and unenforceability of such a contract by alleging that the contract might not be "expressed." *Id*. Obviously, a contract that does not exist is not enforceable. The district court is correct, however, that "the devil is in the details." (App. 152). The district court's determination that a valid contract precluded an unjust enrichment claim was premature and not based on a full assessment of the Appellants' pleading.

CONCLUSION

For the reasons stated herein, the Appellants respectfully request that the judgment of the District Court be reversed and this matter be remanded to commence with discovery and move toward trial by jury on all counts.

Respectfully submitted,

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

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

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

Counsel for Appellants

REQUEST FOR ORAL ARGUMENT

Appellants respectfully request oral argument.

STATUTORY ADDENDUM

5 U.S. CODE § 552A. RECORDS MAINTAINED ON INDIVIDUALS

(a) Definitions.—For purposes of this section—

(1) the term "agency" means agency as defined in section 552(e) [1] of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(8) the term "matching program"—

(A) means any computerized comparison of—

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of—

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs,

or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(B) but does not include—

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

(iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches—

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1));

(ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or

(x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014; 1

(9) the term “recipient agency” means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term “non-Federal agency” means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term “source agency” means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term “Federal benefit program” means any program administered or funded by the Federal Government, or by any agent or State on behalf of the

Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) Conditions of Disclosure.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which

maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

(c) Accounting of Certain Disclosures.—Each agency, with respect to each system of records under its control, shall—

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of

any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to Records.—Each agency that maintains a system of rec-ords shall—

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and—

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either—

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) Agency Requirements.—Each agency that maintains a system of rec-ords shall—

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of rec-ords, which notice shall include—

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) Agency Rules.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if

deemed necessary, for the disclosure to an individual of medical rec-ords, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)

(1) Civil Remedies.—Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)

(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)

(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises,

except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of Legal Guardians.—
For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)

(1) Criminal Penalties.—
Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

(j) General Exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of rec-ords is—

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific Exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of rec-ords is—

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(l)

(1) Archival Records.—

Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m)

(1) Government Contractors.— When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of title 31 shall not be considered a contractor for the purposes of this section.

(n) Mailing Lists.—

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) Matching Agreements.—

(1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program

except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying—

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to—

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel,

that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

(E) procedures for verifying information produced in such matching program as required by subsection (p);

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

(J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and

(K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2)

(A) A copy of each agreement entered into pursuant to paragraph (1) shall—

(i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and

(ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if—

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) Verification and Opportunity to Contest Findings.—

(1) In order to protect any individual whose records are used in a matching program, no recipient agency,non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until—

(A)

(i) the agency has independently verified the information; or

(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that—

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)

(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of—

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) Sanctions.—

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless—

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) Report on New Systems and Matching Programs.—

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) Biennial Report.—The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report—

(1) describing the actions of the Director of the Office of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;

(2) describing the exercise of individual rights of access and amendment under this section during such years;

(3) identifying changes in or additions to systems of records;

(4) containing such other information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t)

(1) Effect of Other Laws.—

No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) Data Integrity Boards.—

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board—

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including—

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)

(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.[2]

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5)

(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that—

(i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;

(ii) there is adequate evidence that the matching agreement will be cost-effective; and

(iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) In the reports required by paragraph (3)(D), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) Responsibilities.—The Director of the Office of Management and Budget shall—

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

(w) Applicability to Bureau of Consumer Financial Protection.—
Except as provided in the Consumer Financial Protection Act of 2010, this section shall apply with respect to the Bureau of Consumer Financial Protection.

28 U.S. CODE § 1291. FINAL DECISIONS OF DISTRICT COURTS

The courts of appeals (other than the United States Court of Appeals for the Federal Circuit) shall have jurisdiction of appeals from all final decisions of the district courts of the United States, the United States District Court for the District of the Canal Zone, the District Court of Guam, and the District Court of the Virgin Islands, except where a direct review may be had in the Supreme Court. The jurisdiction of the United States Court of Appeals for the Federal Circuit shall be limited to the jurisdiction described in sections 1292(c) and (d) and 1295 of this title.

28 U.S. CODE § 1332. DIVERSITY OF CITIZENSHIP; AMOUNT IN CONTROVERSY; COSTS

* * *

(d) (2) The district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which—

(A) any member of a class of plaintiffs is a citizen of a State different from any defendant;

(B) any member of a class of plaintiffs is a foreign state or a citizen or subject of a foreign state and any defendant is a citizen of a State; or

(C) any member of a class of plaintiffs is a citizen of a State and any defendant is a foreign state or a citizen or subject of a foreign state.

* * *

D.C. CODE § 28-3905. COMPLAINT PROCEDURES.

* * *

(k) (2) The remedies or penalties provided by this chapter are cumulative and in addition to other remedies or penalties provided by law. Nothing in this chapter shall prevent any person who is injured by a trade practice in violation of a law of the District of Columbia within the jurisdiction of the Department from exercising any right or seeking any remedy to which the person might be entitled or from filing any complaint with any other agency.

* * *

U.S. CONSTITUTION, ART. III

Section 1.
The judicial power of the United States, shall be vested in one Supreme Court, and in such inferior courts as the Congress may from time to time ordain and establish. The judges, both of the supreme and inferior courts, shall hold their offices during good behaviour, and shall, at stated times, receive for their services, a compensation, which shall not be diminished during their continuance in office.

Section 2.
The judicial power shall extend to all cases, in law and equity, arising under this Constitution, the laws of the United States, and treaties made, or which shall be made, under their authority;--to all cases affecting ambassadors, other public ministers and consuls;--to all cases of admiralty and maritime jurisdiction;--to controversies to which the United States shall be a party;--to controversies between two or more states;--between a state and citizens of another state;--between citizens of different states;--between citizens of the same state claiming lands under grants of different states, and between a state, or the citizens thereof, and foreign states, citizens or subjects.

In all cases affecting ambassadors, other public ministers and consuls, and those in which a state shall be party, the Supreme Court shall have original jurisdiction. In all the other cases before mentioned, the Supreme Court shall have appellate jurisdiction, both as to law and fact, with such exceptions, and under such regulations as the Congress shall make.

The trial of all crimes, except in cases of impeachment, shall be by jury; and such trial shall be held in the state where the said crimes shall have been committed; but when not committed within any state, the trial shall be at such place or places as the Congress may by law have directed.

Section 3.
Treason against the United States, shall consist only in levying war against them, or in adhering to their enemies, giving them aid and comfort. No person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open court.

The Congress shall have power to declare the punishment of treason, but no attainder of treason shall work corruption of blood, or forfeiture except during the life of the person attainted.

UNPUBLISHED DECISION ADDENDUM

OPM Data Security Breach Litigation, Case No. 17-5217 (June 21, 2019)

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued November 2, 2018 Decided June 21, 2019

No. 17-5217

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION,

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, ET AL.,
APPELLEES

NATIONAL TREASURY EMPLOYEES UNION, ET AL.,
APPELLANTS

v.

OFFICE OF PERSONNEL MANAGEMENT, ET AL.,
APPELLEES

Consolidated with 17-5232

Appeals from the United States District Court
for the District of Columbia
(No. 1:15-mc-01394)

Peter A. Patterson argued the cause for Arnold Plaintiffs-Appellants in No. 17-5232. With him on the briefs were *David H. Thompson*, *Daniel C. Girard*, *Jordan Elias*, *Tina Wolfson*, *Gary E. Mason*, and *Richard B. Rosenthal.*

Paras N. Shah argued the cause for appellants National Treasury Employees Union, et al. in No. 17-5217. With him on the briefs were *Gregory O'Duden*, *Larry J. Adkins*, and *Allison C. Giles*.

Marc Rotenberg and *Alan Butler* were on the brief for *amici curiae* Electronic Privacy Information Center (EPIC) and Forty-Four Legal Scholars and Technical Experts in support of appellants.

Sonia M. Carson, Attorney, U.S. Department of Justice, argued the cause for federal appellees. With her on the brief was *Mark B. Stern*.

Jason J. Mendro argued the cause for appellee KeyPoint Government Solutions, Inc. With him on the brief were *F. Joseph Warin*, *Matthew S. Rozen,* and *Jeremy M. Christiansen*.

Alan Charles Raul, *Kwaku A. Akowuah*, *Daniel J. Hay*, and *Steven P. Lehotsky* were on the brief for *amicus curiae* The Chamber of Commerce of the United States of America in support of appellees.

Before: TATEL and MILLETT, *Circuit Judges*, and WILLIAMS, *Senior Circuit Judge*.

Opinion for the Court filed PER CURIAM.

Opinion concurring in part and dissenting in part filed by *Senior Circuit Judge* WILLIAMS.

PER CURIAM: In 2014, cyberattackers breached multiple U.S. Office of Personnel Management ("OPM") databases and allegedly stole the sensitive personal information—including

birth dates, Social Security numbers, addresses, and even fingerprint records—of a staggering number of past, present, and prospective government workers. All told, the data breaches affected more than twenty-one million people. Unsurprisingly, given the scale of the attacks and the sensitive nature of the information stolen, news of the breaches generated not only widespread alarm, but also several lawsuits. These suits were ultimately consolidated into two complaints: one filed by the National Treasury Employees Union and three of its members, and another filed by the American Federation of Government Employees on behalf of several individual plaintiffs and a putative class of others similarly affected by the breaches. Both sets of plaintiffs alleged that OPM's cybersecurity practices were woefully inadequate, enabling the hackers to gain access to the agency's treasure trove of employee information, which in turn exposed plaintiffs to a heightened risk of identity theft and a host of other injuries. The district court dismissed both complaints for lack of Article III standing and failure to state a claim. For the reasons set forth below, we reverse in part and affirm in part.

I

As its name suggests, the U.S. Office of Personnel Management serves as the federal government's chief human resources agency. In that capacity, OPM maintains electronic personnel files that contain, among other information, copies of federal employees' birth certificates, military service records, and job applications identifying Social Security numbers and birth dates.

The agency also oversees more than two million background checks and security clearance investigations per year. To facilitate these investigations, OPM collects a tremendous amount of sensitive personal information from current and prospective federal workers, most of which it then

stores electronically in a "Central Verification System." Consolidated Amended Complaint, *In re United States Office of Pers. Mgmt. Data Security Breach Litig.*, No. 1:15-mc-01394, ¶ 65 (D.D.C. March 14, 2016) ("Arnold Plaintiffs' Compl."), J.A. 61. The investigation-related information stored by OPM includes birth dates, Social Security numbers, residency details, passport information, fingerprints, and other records pertaining to employees' criminal histories, psychological and emotional health, and finances. In recent years, OPM has relied on a private investigation and security firm, KeyPoint Government Solutions, Inc. ("KeyPoint"), to conduct the lion's share of the agency's background and security clearance investigation fieldwork. KeyPoint investigators have access to the information stored in OPM's Central Verification System and can transmit data to and from the agency's network through an electronic portal.

It turns out that authorized KeyPoint investigators have not been the only third parties to access OPM's data systems. Cyberattackers hacked into the agency's network on several occasions between November 2013 and November 2014. Undetected for months, at least two of these breaches resulted in the theft of vast quantities of personal information. According to the complaint, after breaching OPM's network "using stolen KeyPoint credentials" around May 2014, Arnold Plaintiffs' Compl. ¶ 127, J.A. 73, the cyberintruders extracted almost 21.5 million background investigation records from the agency's Central Verification System. They gained access to another OPM system near the end of 2014, stealing over four million federal employees' personnel files. Among the types of information compromised were current and prospective employees' Social Security numbers, birth dates, and residency details, along with approximately 5.6 million sets of fingerprints. The breaches also exposed the Social Security numbers and birth dates of the spouses and cohabitants of those

who, in order to obtain a security clearance, completed a Standard Form 86. According to the complaints, since these 2014 breaches, individuals whose information was stolen have experienced incidents of financial fraud and identity theft; many others whose information has not been misused—at least, not yet—remain concerned about the ongoing risk that they, too, will become victims of financial fraud and identity theft in the future.

After announcing the breaches in the summer of 2015, OPM initially offered individuals whose information had been compromised fraud monitoring and identity theft protection services and insurance at no cost for either eighteen months or three years, depending on whether their Social Security numbers had been exposed. But OPM's offer failed to address the concerns of all such parties, and the agency soon found itself named as a defendant in breach-related lawsuits across the country. The Judicial Panel on Multidistrict Litigation transferred these actions to the U.S. District Court for the District of Columbia for coordinated pretrial proceedings. The suits were ultimately consolidated into two complaints: one brought by the American Federation of Government Employees on behalf of thirty-eight individuals affected by the breaches and a putative class of similarly situated breach victims ("Arnold Plaintiffs") and another for declaratory and injunctive relief brought by the National Treasury Employees Union ("NTEU") and three of its members ("NTEU Plaintiffs"). Below we summarize the relevant allegations and claims contained in each complaint, accepting all factual allegations "as true" and drawing "reasonable inferences * * * in the plaintiffs' favor." *Philipp v. Federal Republic of Germany*, 894 F.3d 406, 409 (D.C. Cir. 2018) (internal quotation marks omitted).

Arnold Plaintiffs allege that KeyPoint's "information security defenses did not conform to recognized industry standards" and that the company unreasonably failed to protect the security credentials that the hackers used to unlawfully access one of OPM's systems in mid-2014. Arnold Plaintiffs' Compl. ¶ 222, J.A. 98. Specifically, they assert that "KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' [personal information] and the credentials used to access it on KeyPoint's and OPM's systems." *Id.* As for OPM, Arnold Plaintiffs allege that the agency had long been on notice that its systems were prime targets for cyberattackers. OPM experienced data breaches related to cyberattacks in 2009 and 2012, and it is no secret that its network is regularly subject to a strikingly large number of hacking attempts. Despite this, say Arnold Plaintiffs, OPM repeatedly failed to comply with the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541 *et seq.* (repealed 2014), and its replacement, the Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551 *et seq.* (collectively, "Information Security Act"), which require agencies to "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." Arnold Plaintiffs' Compl. ¶ 83, J.A. 65.

As early as 2007, Information Security Act compliance audits conducted by OPM's Office of the Inspector General regularly identified major information security deficiencies that left the agency's network vulnerable to attack. Such problems included "severely outdated" security policies and procedures, understaffed and undertrained cybersecurity personnel, and a lack of a centralized information security management structure. Arnold Plaintiffs' Compl. ¶¶ 92–95,

J.A. 67–68. As a result, in every year from 2007 through 2013, the Inspector General identified "serious concerns that * * * pose an immediate risk to the security of assets or operations"—termed "material weaknesses"—in the agency's information security governance program. *Id.* ¶¶ 87–88, J.A. 66; *see also id.* ¶¶ 90–97, J.A. 66–68 (listing those weaknesses). Although in 2014 the Inspector General, acting on the basis of "imminently planned improvements," *id.* ¶ 98, J.A. 68, reclassified OPM's security governance program as a "significant deficiency" (an improvement over the more serious "material weakness"), other serious issues resurfaced at that time. Specifically, in 2014, the agency failed to complete an Information Security Act-required Security Assessment and Authorization for eleven of the twenty-one OPM systems due for reauthorization. Because the agency was unable to ensure the functionality of security controls for the systems that lacked a valid authorization—one of which was "a general system that supported and provided the electronic platform for approximately two-thirds of all information systems operated by OPM"—the Inspector General advised the agency to shut them down. *Id.* ¶¶ 102–103, J.A. 69–70. Despite the Inspector General's recommendation, OPM continued to operate the systems. The agency compounded existing security vulnerabilities by failing to encrypt sensitive data—including Social Security numbers—and failing to enforce multifactor authentication requirements. To make matters worse, when the 2014 data breaches occurred, the agency lacked a centralized network security operations center from which it could continuously and comprehensively monitor all system security controls and threats.

The 2014 cyberattacks were "sophisticated, malicious, and carried out to obtain sensitive information for improper use." Arnold Plaintiffs' Compl. ¶¶ 128, 132, J.A. 73–74. Arnold Plaintiffs assert that as a result of these attacks, they have

suffered from a variety of harms, including the improper use of their Social Security numbers, unauthorized charges to existing credit card and bank accounts, fraudulent openings of new credit card and other financial accounts, and the filing of fraudulent tax returns in their names. At least three named Arnold Plaintiffs purchased credit monitoring services after falling victim to such fraud; others have spent time and money attempting to unwind fraudulent transactions made in their names. And some Arnold Plaintiffs who have yet to experience a fraud incident purchased credit monitoring services and spent extra time monitoring their accounts to mitigate the "increased risk" of identity theft caused by the breaches. *Id.* ¶ 163, J.A. 81–83.

Arnold Plaintiffs assert several claims against OPM, but they press only one on appeal: that the agency "willfully failed" to establish appropriate safeguards to ensure the security and confidentiality of their private information, in violation of Section 552a(e)(10) of the Privacy Act of 1974. Arnold Plaintiffs' Compl. ¶ 182, J.A. 89; *see also* 5 U.S.C. § 552a(e)(10) (requiring the agency to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained"). They also bring a variety of common-law and statutory claims against KeyPoint, alleging that the company's "actions and inactions constitute[d] negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and state statutes." Arnold Plaintiffs' Compl. ¶ 9, J.A. 38. Arnold Plaintiffs seek damages from OPM under the Privacy Act; from KeyPoint, they request money damages and an order requiring the company to extend

free lifetime identity theft and fraud protection services to all putative class members, among other things.

The other complaint, filed by the National Treasury Employees Union, seeks declaratory and injunctive relief against the Acting Director of OPM in her official capacity based on essentially the same set of facts. NTEU Plaintiffs assert that when they provided OPM with the sensitive personal information ultimately exposed in the breaches, they did so upon the agency's assurance that it "would be safeguarded" and kept confidential. Amended Complaint for Declaratory and Injunctive Relief, *In re United States Office of Pers. Mgmt. Data Security Breach Litig.*, No. 1:15-mc-01394, ¶ 75 (D.D.C. June 3, 2016) ("NTEU Plaintiffs' Compl."), J.A. 179. They allege that OPM's "reckless failure to safeguard [NTEU Plaintiffs'] personal information," which ultimately "resulted in [its] unauthorized disclosure" during the 2014 attacks, *id.* at 3, J.A. 155, amounted to a violation of what they describe as their "constitutional right to informational privacy," *id.* ¶ 98, J.A. 186.

NTEU Plaintiffs further allege that, despite the fallout from the 2014 breaches, OPM has yet to make the cybersecurity improvements necessary to protect their personal information from future attacks. According to the complaint, the agency's Inspector General warned at the end of 2015 that OPM was ill-equipped to protect itself from another attack, given "the overall lack of compliance that seems to permeate the agency's IT security program." NTEU Plaintiffs' Compl. ¶ 88, J.A. 182 (quoting United States Office of Pers. Mgmt., Office of the Inspector General, Office of Audits, *Final Audit Report: Federal Information Security Modernization Act Audit FY 2015*, at 5 (Nov. 10, 2015)). NTEU Plaintiffs seek a declaration that OPM's failure to protect their information violated their putative constitutional right to informational

privacy and an order requiring the agency to provide them with free lifetime credit monitoring and identity theft protection. They also request an injunction requiring OPM "to take immediately all necessary and appropriate steps to correct deficiencies in [its] IT security program so that NTEU members' personal information will be protected from unauthorized disclosure" in the future. *Id.* at 35, J.A. 187.

OPM and KeyPoint moved to dismiss Arnold Plaintiffs' complaint, arguing that they lacked Article III standing, that their claims were barred by sovereign immunity, and that they failed to state valid claims under the state and federal statutes and common-law theories invoked. OPM moved to dismiss NTEU Plaintiffs' complaint for lack of standing and failure to state a claim upon which relief could be granted—that is, failure to allege a cognizable constitutional violation. The district court granted both motions to dismiss on the ground that neither Arnold Plaintiffs nor NTEU Plaintiffs pled sufficient facts to demonstrate Article III standing. Rejecting plaintiffs' argument that they faced a heightened risk of identity theft due to the breaches, the court held that the facts alleged failed to plausibly support the conclusion that this risk of future injury was either substantial or clearly impending. The district court ultimately concluded that only those plaintiffs who specifically identified out-of-pocket losses stemming from the actual misuse of their data had suffered an injury in fact sufficient for standing purposes. But even those plaintiffs lacked standing, the district court concluded, because they failed to allege facts demonstrating that the misuse of their information was traceable to the OPM breaches in particular.

The district court went on to explain that it also lacked subject matter jurisdiction over Arnold Plaintiffs' claims for the additional reasons that (i) they failed to plead the actual damages necessary to bring them within the Privacy Act's

waiver of sovereign immunity; and (ii) as a government contractor, KeyPoint enjoyed derivative sovereign immunity from suit. Finally, the court concluded that Arnold Plaintiffs failed to plausibly allege a Privacy Act claim and that NTEU Plaintiffs' complaint failed to state a constitutional claim. Both sets of plaintiffs have appealed.

We reverse in part and affirm in part the district court's judgment. We hold that both sets of plaintiffs have alleged facts sufficient to satisfy Article III standing requirements. Arnold Plaintiffs have stated a claim for damages under the Privacy Act, and have unlocked OPM's waiver of sovereign immunity, by alleging OPM's knowing refusal to establish appropriate information security safeguards. KeyPoint is not entitled to derivative sovereign immunity because it has not shown that its alleged security faults were directed by the government, and it is alleged to have violated the Privacy Act standards incorporated into its contract with OPM. Finally, we agree with the district court that, assuming a constitutional right to informational privacy, NTEU Plaintiffs have not alleged any violation of such a right.

II

"[T]he irreducible constitutional minimum of standing consists of three elements." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (internal quotation marks omitted). First, plaintiffs must demonstrate that they suffered an injury in fact that is "concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 1548 (internal quotation marks omitted). "An allegation of future injury" passes Article III muster only if it "is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013)). Second, plaintiffs must demonstrate causation; that is, they must show

that their claimed injury is "fairly traceable to the challenged conduct of the defendant." *Spokeo*, 136 S. Ct. at 1547. "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018). And third, plaintiffs must demonstrate that "it is likely, as opposed to merely speculative, that the[ir] injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Environmental Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000).

Where, as here, defendants challenge standing at the pleading stage without disputing the facts alleged in the complaint, "we accept the well-pleaded factual allegations as true and draw all reasonable inferences from those allegations in the plaintiff's favor," but we do not assume the truth of legal conclusions or accept inferences that are unsupported by the facts alleged in the complaint. *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015). "We review de novo the district court's dismissal for lack of standing." *Id.* The question at this early juncture in the litigation is whether plaintiffs have plausibly alleged standing. Contrary to the district court's ruling, plaintiffs need not yet establish each element of standing by a preponderance of the evidence. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.,* with the manner and degree of evidence required at the successive stages of the litigation.").

A

We begin with NTEU Plaintiffs. For standing purposes, we assume that NTEU Plaintiffs have, as they claim, a "constitutional right to informational privacy" that was

violated "the moment that [cyberattackers stole] their inherently personal information * * * from OPM's deficiently secured databases." NTEU Br. 11; *see also Estate of Boyland v. Department of Agric.*, 913 F.3d 117, 123 (D.C. Cir. 2019) ("[W]hen considering whether a plaintiff has Article III standing, a federal court must assume, *arguendo*, the merits of his or her legal claim.") (internal quotation marks omitted). Furthermore, given NTEU Plaintiffs' allegations regarding OPM's continued failure to adequately secure its databases, it is reasonable to infer that there remains a "substantial risk" that their personal information will be stolen from OPM again in the future. NTEU Plaintiffs' Compl. ¶ 88, J.A. 182. With respect to this claim, the loss of a constitutionally protected privacy interest itself would qualify as a concrete, particularized, and actual injury in fact. And the ongoing and substantial threat to that privacy interest would be a concrete, particularized, and *imminent* injury in fact. Both claimed injuries are plausibly traceable to OPM's challenged conduct, and the latter is redressable either by a declaration that the agency's failure to protect NTEU Plaintiffs' personal information is unconstitutional or by an order requiring OPM to immediately correct deficiencies in its cybersecurity programs. *Cf. ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (holding that, where plaintiffs allege a Fourth Amendment "injury [stemming] from the very collection of their telephone metadata," they "have suffered a concrete and particularized injury fairly traceable to the challenged program and redressable by a favorable ruling"). Accordingly, NTEU Plaintiffs have standing based on their claimed constitutional injury.

B

Arnold Plaintiffs allege no such constitutional injury, but they do claim to have suffered a variety of past and future data-breach related harms. *See, e.g.*, Arnold Plaintiffs' Compl. ¶ 22,

J.A. 44–45 (alleging that Plaintiff Jane Doe has "suffer[ed] stress resulting from concerns for her personal safety and that of her family members" since being informed by the FBI that her personal information "had been acquired by the so-called Islamic State of Iraq and al-Sham ('ISIS')"). For purposes of our standing analysis, we focus on one injury they all share: the risk of future identity theft. As we have already recognized, "identity theft * * * constitute[s] a concrete and particularized injury." *Attias*, 865 F.3d at 627; *see also Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (offering the "increased risk of fraud or identity theft" as an "example" of a "concrete consequence" for standing purposes). Yet, the district court concluded that Arnold Plaintiffs' complaint provided an insufficient basis from which to infer that, in the wake of the OPM breaches, Arnold Plaintiffs faced any meaningful risk of future identity theft, much less a "substantial" one. *In re United States Office of Pers. Mgmt. Data Security Breach Litig.* ("*In re OPM*"), 266 F. Supp. 3d 1, 35 (D.D.C. 2017). Furthermore, finding that "the risk of identity theft was neither clearly impending nor substantial," the district court concluded that any expenses that Arnold Plaintiffs incurred attempting to mitigate that risk likewise failed to qualify as an Article III injury in fact. *Id.* at 36; *see also Clapper*, 568 U.S. at 416 ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

Arnold Plaintiffs argue that the district court's conclusion is incompatible with our decision in *Attias v. CareFirst*. In that case, we determined that the victims of a cyberattack on CareFirst, a health insurance company, "cleared the low bar to establish their standing at the pleading stage" by plausibly alleging that they faced a substantial risk of identity theft as a result of the company's negligent failure to thwart the attack.

Attias, 865 F.3d at 622. Specifically, the complaint alleged that the breach exposed "all of the information wrongdoers need for appropriation of a victim's identity": personal identification information, credit card numbers, and Social Security numbers. *Id.* at 628 (internal quotation marks omitted). Based largely on the nature of the information compromised in the attack, we concluded that it was reasonable to infer that the cyberattackers had "both the intent and the ability to use that data for ill." *Id.*; *see also id.* at 628–629 ("Why else would hackers break into a * * * database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.") (quoting *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015)). Accordingly, we explained, "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629.

Although the OPM cyberattacks differ in several respects from the breach at issue in *Attias*, there is no question that the OPM hackers, too, now have in their possession all the information needed to steal Arnold Plaintiffs' identities. Arnold Plaintiffs have alleged that the hackers stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information. It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft. Indeed, several Arnold Plaintiffs claim that they have already experienced various types of identity theft, including the unauthorized opening of new credit card and other financial accounts and the filing of fraudulent tax returns in their names. Moreover, unlike existing credit card numbers, which, if compromised, can be changed to prevent future fraud, Social Security numbers and

addresses cannot so readily be swapped out for new ones. And, of course, our birth dates and fingerprints are with us forever. Viewing the allegations in the light most favorable to Arnold Plaintiffs, as we must, we conclude that not only do the incidents of identity theft that have already occurred illustrate the nefarious uses to which the stolen information may be put, but they also support the inference that Arnold Plaintiffs face a substantial—as opposed to a merely speculative or theoretical—risk of future identity theft.

It is worth noting that several Arnold Plaintiffs also allege that unauthorized charges have appeared on their existing credit card and bank account statements since the breaches. According to OPM, because none of these Arnold Plaintiffs "specifically alleged the OPM incidents affected their existing account information," the reported incidents of fraud on existing accounts (and, presumably, the risk of future fraud on those accounts) cannot plausibly be attributed to the OPM breaches. Gov't Br. 21. But we need not travel down that road because, regardless of whether the hackers obtained all the information necessary to make unauthorized charges to existing accounts, it is undisputed that the other forms of fraud alleged—the opening of new accounts and the filing of fraudulent tax returns—may be accomplished using the information stolen during the breaches at issue.

OPM argues that Arnold Plaintiffs' allegations of "scattered instances of widely varying fraud" are insufficient to support a plausible inference that Arnold Plaintiffs face an ongoing, substantial risk of identity theft. Gov't Br. 20. Specifically, OPM contends that despite the sensitive nature of the information stolen in the attacks, "[i]t is impossible under these circumstances to 'easily construct any kind of colorable theory' that a desire to commit fraud motivated" the OPM breaches. *Id.* at 21 (quoting *In re OPM*, 266 F. Supp. 3d at 38).

This is especially the case, OPM argues, because "this is not just a data breach," but rather "a data breach arising out of a particular sort of cyberattack" against the United States. *Id.* at 23 (quoting *In re OPM*, 266 F. Supp. 3d at 9). According to OPM, it is illogical to assume that the same goals that typically motivate hackers of commercial databases animated the "sophisticated" actors who engineered these data breaches. *Id.* at 27. The district court agreed with OPM on this point. Although neither amended complaint contains any allegations regarding the cyberattackers' identity, the court noted that news articles and congressional reports had suggested that the suspected perpetrator was not a common criminal, but rather the Chinese government. Despite acknowledging that "a finding concerning the source of the breach" was "beyond the scope of [the] proceeding at this juncture," the court appears to have relied at least partially on this external information in reaching the conclusion that it was implausible that the OPM hackers intended to steal Arnold Plaintiffs' identities. *In re OPM*, 266 F. Supp. 3d at 34.

As an initial matter, the district court should not have relied even in part on its own surmise that the Chinese government perpetrated these attacks. Absent any factual allegations regarding the identity of the cyberattackers, the district court was not free to conduct its own extra-record research and then draw inferences from that research in OPM's and KeyPoint's favor. *See Arpaio*, 797 F.3d at 19 (explaining that where the defendant challenges the plaintiff's standing at the motion-to-dismiss stage, we "draw all reasonable inferences * * * in the plaintiff's favor"). Beyond that, although a cyberattack on a government system might well be motivated by a purpose other than identity theft, given the type of information stolen in the OPM breaches and Arnold Plaintiffs' allegations regarding the subsequent misuse of that information, it is just as plausible to infer that identity theft is

at least one of the hackers' goals, even if those hackers are indeed affiliated with a foreign government.

Our dissenting colleague takes a different tack, suggesting that because this case involves *government* databases, "espionage * * * is * * * an 'obvious alternative explanation'" for the attacks. *See* Dissenting Op. at 4 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 682 (2009)). We disagree as to just how obvious an explanation this is based on the facts alleged in the complaint. Furthermore, given that espionage and identity theft are not mutually exclusive, the likely existence of an espionage-related motive hardly renders implausible Arnold Plaintiffs' claim that they face a substantial future risk of identity theft and financial fraud as a result of the breaches. *See, e.g.*, *Watson Carpet & Floor Covering, Inc. v. Mohawk Indus., Inc.*, 648 F.3d 452, 458 (6th Cir. 2011) ("Ferreting out the most likely reason for the defendants' actions is not appropriate at the pleadings stage * * * . [T]he plausibility of [one particular] reason for the refusals to sell carpet does not render all other reasons implausible."). By contrast, in the cases cited by the dissent, the obvious alternative explanations were necessarily incompatible with the plaintiffs' versions of events. *See Iqbal*, 556 U.S. at 682 (rejecting claims of invidious discrimination as implausible where there existed an obvious, nondiscriminatory law enforcement justification for the challenged acts); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 567–568 (2007) (rejecting a conspiracy claim as implausible where history and market forces provided "a natural explanation" for the defendants' behavior).

In any case, although we found in *Attias* that the circumstances of that breach made it at least plausible that the hackers there had "both the intent and the ability to use [the plaintiffs'] data for ill," 865 F.3d at 628, a hacker's "intent" to use breach victims' personal data for identity theft becomes

markedly less important where, as here, several victims allege that they have *already* suffered identity theft and fraud as a result of the breaches. When considered in combination with the obvious potential for fraud presented by the information stolen during the breaches, the fact that certain Arnold Plaintiffs have already had fraudulent accounts opened and tax returns filed in their names moves the risk of future identity theft across the line from speculative to substantial, at least at this early stage in the proceedings. *See id.* at 625 (explaining that at the pleading stage, "plaintiffs are required only to state a *plausible* claim that each of the standing elements is present") (internal quotation marks omitted).

The circumstances here differ markedly from those in the two cases OPM cites in support of its argument that Arnold Plaintiffs' risk of future identity theft is merely conjectural. In *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), a laptop containing patients' unencrypted personal information, "including names, birth dates, the last four digits of social security numbers, and physical descriptors," and four boxes of medical records that contained names and Social Security numbers went missing from a Veterans Affairs medical center. *Id.* at 267–269. The Fourth Circuit held that the risk of future identity theft stemming from the incidents was too speculative to satisfy the injury-in-fact requirement because the plaintiffs failed to allege either (i) that the thief "intentionally targeted" the personal information contained in the laptop and boxes or (ii) that the thief subsequently used that information to commit identity theft. *Id.* at 274–275 ("[E]ven after extensive discovery, the * * * plaintiffs [who sued over the theft of the laptop] have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."); *id.* at 275 ("Watson's complaint suffers from

the same deficiency with regard to the four missing boxes of pathology reports."). Without such allegations, the Fourth Circuit explained, there was nothing to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274.

In the other case, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), an unknown hacker infiltrated a payroll processing firm's database, "potentially" gaining access to employees' "personal and financial information." *Id.* at 40. It was "not known whether the hacker read, copied, or understood the data," *id.*, and none of the affected parties alleged that their data had since been misused, *id.* at 44 ("Appellants have alleged no misuse."). Because the plaintiffs' claimed risk of future identity theft therefore rested solely on "hypothetical speculations concerning the possibility of future injury," the Third Circuit held that the risk was insufficient to support standing. *Id.* at 43.

Here, in contrast to those two cases, Arnold Plaintiffs both allege that the OPM cyberattackers intentionally targeted their information and point out the subsequent misuse of that information. *See* Arnold Plaintiffs' Compl. ¶¶ 128, 130, J.A. 73–74 (alleging that the hackers targeted—and extracted data from—the agency's "Electronic Official Personnel Folder system" and the database used to collect background check information); *see, e.g.*, *id.* ¶¶ 21–22, 24, 26, J.A. 44–48 (alleging incidents involving misuse of information). These are precisely the types of allegations missing in *Beck* and *Reilly*. *See Beck*, 848 F.3d at 275 ("[T]he mere theft of these items, *without more*, cannot confer Article III standing.") (emphasis added); *Reilly*, 664 F.3d at 44 ("Here, there is no evidence that the intrusion was intentional or malicious. Appellants have alleged no misuse * * * . Indeed, no

identifiable taking occurred; all that is known is that a firewall was penetrated.").

Although it is true, as a general principle, that "'as * * * breaches fade further into the past,' * * * threatened injuries become more and more speculative," we are unpersuaded by the dissent's suggestion that the passage of less than two years between these particular attacks and Arnold Plaintiffs' filing of the operative complaint is enough to render the threat of future harm insubstantial. Dissenting Op. at 7 (quoting *Beck*, 848 F.3d at 275). The plaintiffs in *Beck* suffered no misuse of their data prior to filing their complaint. *See supra* at 19–20. And the same was true of the plaintiffs in *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564 (D. Md. 2016), the case cited by the dissent and the court in *Beck* for the proposition that the threat of future injury diminishes over time. *See id.* at 570 (noting that plaintiffs had not experienced "*any* misuse" of their data prior to filing their complaint). Although the passage of two years in a run-of-the-mill data breach case might, absent allegations of subsequent data misuse, suggest that a claim of future injury is less than plausible, that is not the situation we face here. Conducted over several months by sophisticated and apparently quite patient cyberhackers, the attacks at issue in this case affected over twenty-one million people and involved information far more sensitive than credit card numbers. Cyberhacking on such a massive scale is a relatively new phenomenon, and we are unwilling at this stage to assume that the passage of a year or two without any clearly identifiable pattern of identity theft or financial fraud means that all those whose data was compromised are in the clear.

Drawing all reasonable inferences in Arnold Plaintiffs' favor, we conclude that they have alleged facts sufficient to support their claim of future injury, notwithstanding the passage of time and the governmental character of the

databases at issue here. Given the nature of the information stolen and the fact that several named Arnold Plaintiffs have already experienced some form of identity theft since the breaches, it is at least plausible that Arnold Plaintiffs run a substantial risk of falling victim to other such incidents in the future. *See Hutton v. National Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621–622 (4th Cir. 2018) (finding a substantial risk of identity theft where the plaintiffs alleged not only that their information had been stolen by hackers, but also that it was subsequently "used in a fraudulent manner"). Because Arnold Plaintiffs adequately allege a substantial risk of future identity theft, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact. *See id.* at 622 ("[T]he [Supreme] Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists.") (citing *Clapper*, 568 U.S. at 414 n.5); *see also* Hearing Tr. 35 (Oct. 27, 2016) (credit protection services for victims of the breaches announced in June 2015 were not "up and running until September" of that year); Arnold Plaintiffs' Compl. ¶ 28, J.A. 48–49 (Plaintiff Kelly Flynn purchased credit monitoring in July 2015).

The district court evaluated the second element of Article III standing, causation, only as to the incidents of identity theft and fraud that Arnold Plaintiffs had already experienced. Observing that such incidents were "separated across time and geography, and they follow no discernable pattern," *In re OPM*, 266 F. Supp. 3d at 38, the court determined that it could not reasonably infer causation because Arnold Plaintiffs had not alleged "any facts that plausibly connect the various isolated incidents of the misuse * * * to the breaches at issue here," *id.* at 37. The district court did not go on to consider whether Arnold Plaintiffs plausibly alleged that a risk of *future* identity theft was fairly traceable to OPM's and KeyPoint's

cybersecurity failings, presumably because it had already rejected that risk as merely speculative. We can make relatively short work of such an inquiry here.

Arnold Plaintiffs have alleged facts supporting a reasonable inference that their claimed data breach-related injuries are fairly traceable to OPM's failure to secure its information systems. Not only do Arnold Plaintiffs detail OPM's failure to heed repeated warnings by its own Inspector General regarding serious vulnerabilities in the agency's systems, but they also allege that as a result of that failure, hackers managed to breach key OPM systems on several different occasions.

With respect to KeyPoint, Arnold Plaintiffs further allege that the company's failure to properly secure its login credentials "was a substantial factor in causing the Data Breaches." Arnold Plaintiffs' Compl. ¶ 228, J.A. 99. KeyPoint contends that Arnold Plaintiffs' complaint fails to trace the breaches to any actual misconduct by KeyPoint, but that argument lacks merit. Arnold Plaintiffs' complaint alleges not only that the hackers accessed OPM's systems "using stolen KeyPoint credentials," *id.* ¶ 127, J.A. 73, but also that the company was negligent in "failing to protect and secure its * * * credentials," *id.* ¶ 228, J.A. 99, by, among other things, "failing to * * * comply with industry-standard data security practices," *id.* ¶ 223(b), J.A. 98. It is reasonable to infer that "data security practices" would cover practices related to securing credentials. It is likewise reasonable to infer, based on the allegations contained in the complaint, that KeyPoint is at least partially to blame for the breaches due to its failure to comply with such practices.

As previously explained, even if the breaches in question did not expose all information necessary to make fraudulent

charges on victims' existing financial accounts, the personal data the hackers did manage to obtain is enough, by itself, to enable several forms of identity theft. That fact, combined with the allegations that at least some of the stolen information was actually misused after the breaches, suffices to support a reasonable inference that Arnold Plaintiffs' risk of future identity theft is traceable to the OPM cyberattacks. Neither the likelihood that some Arnold Plaintiffs experienced other types of unrelated fraud nor the speculative possibility that they might also have been the victims of other data breaches renders causation implausible here. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) ("That hackers might have stolen Plaintiffs' [personal identifying information] in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches * * *, is less about standing and more about the merits of causation and damages."), *cert. denied*, 139 S. Ct. 1373 (2019). Nor are we troubled, as OPM suggests we should be, by certain Arnold Plaintiffs' failure to specify exactly when, in relation to the data breaches, fraudsters first misused their data. The Supreme Court has explained that "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Lujan*, 504 U.S. at 561 (formatting altered). Accordingly, as in *Attias*, at this early stage, we have "little difficulty concluding," 865 F.3d at 629, that Arnold Plaintiffs have met their "relatively modest" burden of alleging that their risk of future identity theft is fairly traceable to OPM's and KeyPoint's challenged conduct, *Bennett v. Spear*, 520 U.S. 154, 171 (1997).

This brings us, then, to the final element of standing, where, as previously noted, we ask whether "it is likely, as opposed to merely speculative" that Arnold Plaintiffs' claimed

injury "will be redressed by a favorable decision." *Friends of the Earth*, 528 U.S. at 181. Although the district court never reached this question, we think Arnold Plaintiffs have easily demonstrated that their substantial risk of future identity theft and related mitigation expenses are redressable.

Granting that it may well be impossible at this point to eliminate the risk of future identity theft stemming from the OPM breaches, the money damages Arnold Plaintiffs seek can redress certain proven injuries related to that risk (such as reasonably-incurred credit monitoring costs). *See, e.g.*, *In re Zappos.com*, 888 F.3d at 1030 ("The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages.") (citation omitted); *Attias*, 865 F.3d at 629 ("The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages.").

In sum, like the *Attias* plaintiffs, both sets of plaintiffs here have "cleared the low bar to establish their standing at the pleading stage." 865 F.3d at 622. Arnold Plaintiffs have plausibly alleged a substantial risk of future identity theft that is fairly traceable to OPM's and KeyPoint's cybersecurity failings and likely redressable, at least in part, by damages, and NTEU Plaintiffs have plausibly alleged actual and imminent constitutional injuries that are likewise traceable to OPM's challenged conduct and redressable either by a declaration that the agency's failure to protect plaintiffs' personal information is unconstitutional or by an order requiring OPM to correct deficiencies in its cybersecurity program. We therefore have no need to address the other bases for standing asserted by NTEU and Arnold Plaintiffs. *See, e.g.*, *id.* at 626 n.2 (explaining that when plaintiffs have standing "based on their

heightened risk of future identity theft," it is unnecessary to address their other theories of injury in fact).

Having resolved the standing issue in NTEU and Arnold Plaintiffs' favor, we turn to another potential jurisdictional stumbling block: sovereign immunity.

III

It is "axiomatic" that a waiver of sovereign immunity is a jurisdictional "prerequisite" for Arnold Plaintiffs' claims against OPM to get out of the starting gate. *United States v. Mitchell*, 463 U.S. 206, 212 (1983); *accord Federal Deposit Ins. Corp. v. Meyer*, 510 U.S. 471, 475 (1994). The Privacy Act, 5 U.S.C. § 552a, provides just such a waiver of sovereign immunity. That statute "safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records." *Henke v. Department of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996) (quoting *Bartel v. Federal Aviation Admin.*, 725 F.2d 1403, 1407 (D.C. Cir. 1984)). As part of that obligation, the Act mandates that federal agencies "protect the privacy of individuals identified in information systems maintained by [them]." Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896, 1896 (1974). The Privacy Act waives sovereign immunity by expressly authorizing a cause of action for damages against federal agencies that violate its rules protecting the confidentiality of private information in agency records. *See Tomasello v. Rubin*, 167 F.3d 612, 617–618 (D.C. Cir. 1999).

The district court nonetheless ruled that OPM's sovereign immunity remained intact, reasoning that Arnold Plaintiffs failed to allege the type of harms covered by the Privacy Act. Reviewing the district court's dismissal of the Privacy Act claim *de novo*, *Skinner v. Department of Justice*, 584 F.3d

1093, 1096 (D.C. Cir. 2009), we reverse. OPM's allegedly willful failure to protect Arnold Plaintiffs' sensitive personal information against the theft that occurred falls squarely within the Privacy Act's ambit.

To unlock the Privacy Act's waiver of sovereign immunity and state a cognizable claim for damages, a plaintiff must allege that (i) the agency "intentional[ly] or willful[ly]" violated the Act's requirements for protecting the confidentiality of personal records and information; and (ii) she sustained "actual damages" (iii) "as a result of" that violation. 5 U.S.C. § 552a(g)(4); *see Chichakli v. Tillerson*, 882 F.3d 229, 233 (D.C. Cir. 2018). At this threshold stage of the litigation, Arnold Plaintiffs have plausibly alleged each of those elements.

A

To start, Arnold Plaintiffs have straightforwardly alleged a "willful" violation of the Privacy Act's requirements. 5 U.S.C. § 552a(g)(4). OPM was necessarily aware that the Privacy Act requires it to "establish appropriate administrative, technical, and physical safeguards" that "insure the security and confidentiality of records," and to "protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a(e)(10).

The complaint alleges in no uncertain terms that OPM dropped that ball because appropriate safeguards were not in place. *See, e.g.*, Arnold Plaintiffs' Compl. ¶ 134, J.A. 74 ("OPM's decisions not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year

without being detected."); *id.* ¶ 178, J.A. 87 ("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' [government investigation information] under OPM's control was exposed, stolen, and misused.").

Of course, violating the Privacy Act is not by itself enough. The agency's transgression must have been "intentional or willful." 5 U.S.C. § 552a(g)(4). Under the Privacy Act, willfulness means more than "gross negligence." *Maydak v. United States*, 630 F.3d 166, 179 (D.C. Cir. 2010); *see also Coleman v. United States*, 912 F.3d 824, 836–837 (5th Cir. 2019) ("at least gross negligence"); *Beaven v. Department of Justice*, 622 F.3d 540, 549 (6th Cir. 2010) ("something greater than gross negligence"); *Hogan v. England*, 159 F. App'x 534, 537 (4th Cir. 2005) ("somewhat greater than gross negligence") (formatting altered); *Johnston v. Horne*, 875 F.2d 1415, 1422 (9th Cir. 1989) ("conduct amounting to more than gross negligence"), *overruled on other grounds*, *Irwin v. Department of Veterans Affairs*, 498 U.S. 89 (1990). Allegations that the agency's conduct was "disjointed" or "confused," or that errors were "inadvertent[]" will not suffice. *Maydak*, 630 F.3d at 180 (internal quotation marks omitted).

Instead, a complaint must plausibly allege that the agency's security failures were "in flagrant disregard of [their] rights under the Act," were left in place "without grounds for believing them to be lawful," or were "so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful." *Maydak*, 630 F.3d at 179; *accord* 120 Cong. Rec. 40406 (1974) ("Analysis of House and Senate Compromise Amendments to the Federal Privacy Act") ("On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed

as only somewhat greater than gross negligence."); *see also Beaven*, 622 F.3d at 549 (requiring defendants to have "committ[ed] the act without grounds for believing it to be lawful, or flagrantly disregard[ed] others' rights under the Privacy Act") (formatting altered); *Andrews v. Veterans Admin.*, 838 F.2d 418, 425 (10th Cir. 1988) (agency "action [must be] so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful, or conduct committed without grounds for believing it to be lawful or [an] action flagrantly disregarding others' rights under the Act") (formatting altered).[1]

Arnold Plaintiffs' complaint clears that hurdle by plausibly and with specificity alleging that OPM was willfully indifferent to the risk that acutely sensitive private information was at substantial risk of being hacked. According to the complaint, at the time of the breach, OPM had long known that its electronic record-keeping systems were prime targets for hackers. The agency suffered serious data breaches from hackers in 2009 (millions of users' personal information stolen) and 2012 (OPM access credentials stolen and posted online), and is subject to at least *ten million* unauthorized electronic

[1] *Cf. McLaughlin v. Richland Shoe Co.*, 486 U.S. 128, 132–133 (1988) ("willful" under the Fair Labor Standards Act includes "reckless[]" violations); *Trans World Airlines, Inc. v. Thurston*, 469 U.S. 111, 126 (1985) (willfulness in the Age Discrimination in Employment Act includes "reckless disregard for the matter of whether [the defendant's] conduct was prohibited by" the Act); *United States v. Murdock*, 290 U.S. 389, 395 (1933) ("willful" violation of the Revenue Acts of 1926 and 1928 is "marked by careless disregard [for] whether or not one has the right so to act"); *Dayton Tire v. Secretary of Labor*, 671 F.3d 1249, 1254 (D.C. Cir. 2012) (willful violation of the Occupational Safety and Health Act is "an act done voluntarily with either an intentional disregard of, or plain indifference to, the Act's requirements").

intrusion attempts *every month*. Arnold Plaintiffs' Compl. ¶¶ 78–79, J.A. 64.

Despite that pervading threat, OPM effectively left the door to its records unlocked by repeatedly failing to take basic, known, and available steps to secure the trove of sensitive information in its hands. Information Security Act audits by OPM's Inspector General repeatedly warned OPM about material deficiencies in its information security systems. Among the identified flaws were

- severely outdated security policies and procedures;
- permitting employees to leave open, or to not terminate, remote access;
- understaffed and undertrained cybersecurity personnel;
- failure to implement or enforce multi-factor identification in *any* of its major information systems;
- declining to patch or install security updates for its systems promptly;
- lacking a mature vulnerability scanning program to find and track the status of security weaknesses in its systems;
- failure to maintain a centralized information security management structure that would continuously monitor security events and controls;
- lacking the ability to detect unauthorized devices connected to its network; and
- failure to engage in appropriate oversight of its contractor-operated systems.

So forewarned, OPM chose to leave those critical information security deficiencies (and more) in place. On top of that, in the year that the hacks occurred, OPM (allegedly)

also left undone mandated security assessments and authorizations for half of its electronic record-keeping systems. 44 U.S.C. § 3554(b); *id.* § 3544(b) (repealed 2014); Arnold Plaintiffs' Compl. ¶¶ 101–102, J.A. 69 (no information security assessments conducted for eleven of the twenty-one systems). The risk created by these lapses was so serious that the Inspector General took the unprecedented step of advising OPM to shut down all the systems lacking valid authorizations until adequate security measures could be put in place. OPM declined, choosing instead to continue operating these systems.

The complaint's plausible allegations that OPM decided to continue operating in the face of those repeated and forceful warnings, without implementing even the basic steps needed to minimize the risk of a significant data breach, is precisely the type of willful failure to establish appropriate safeguards that makes out a claim under the Privacy Act. *See American Fed'n of Gov't Employees v. Hawley*, 543 F. Supp. 2d 44, 52 (D.D.C. 2008) (Department of Homeland Security's failure to establish appropriate safeguards to prevent losing a computer hard drive was "intentional and willful" given the Inspector General's repeated warnings of "recurring, systemic, and fundamental deficiencies" in the agency's information security); *In re Department of Veterans Affairs (VA) Data Theft Litig.*, No. 06–0506 (JR), 2007 WL 7621261, at *4–5 (D.D.C. Nov. 16, 2007) (Department of Veterans Affairs' failure to establish appropriate safeguards to protect against theft of laptop and hard drive was "intentional and willful" in light of the Government Accountability Office's repeated warnings of "deficiencies" in the agency's "information security").

B

Arnold Plaintiffs' lawsuit is not in the clear yet. The complaint must also allege facts showing that they suffered

"actual damages" as "a result of" OPM's Privacy Act violation. 5 U.S.C. § 552a(g)(4). The complaint rises to that task as well.

1

"Actual damages" within the meaning of the Privacy Act are limited to proven pecuniary or economic harm. *Federal Aviation Admin. v. Cooper*, 566 U.S. 284, 298–299 (2012). The district court concluded that only two Arnold Plaintiffs had properly alleged that they suffered "actual damages": Jane Doe, who incurred legal fees when she retained a law firm to close fraudulent accounts opened in her name, and Charlene Oliver, whose electricity account had been fraudulently accessed and saddled with unauthorized charges.

While those harms certainly qualify as actual damages, the complaint contains still more relevant allegations of injury.

First, nine of the named Arnold Plaintiffs purchased credit protection and/or credit repair services after learning of the breach. Paul Daly, for example, purchased credit monitoring services after a fraudulent 2014 tax return was filed in his name. And Teresa J. McGarry subscribed to a monthly credit and identity protection service to prevent identity theft. Those reasonably incurred out-of-pocket expenses are the paradigmatic example of "actual damages" resulting from the violation of privacy protections. *See Cooper*, 566 U.S. at 298.[2]

OPM counters that those individual purchases were unnecessary because Congress provided credit monitoring

[2] Congress authorized the expenditure of hundreds of millions of taxpayer dollars to purchase ten years' worth of fraud and credit monitoring services to protect victims of the data breach. *See* Consolidated Appropriations Act, Pub. L. No. 115-31, § 633(a), 131 Stat. 135, 376 (2017).

services for potentially affected individuals. Congress, though, did not offer credit repair services. Anyhow, the argument wrongly assumes facts in OPM's favor at the complaint stage, such as that the services offered were equal or superior to those obtained privately, or that they took effect in a timely manner and for a sufficient period of time. *See Agnew v. District of Columbia*, 920 F.3d 49, 53 (D.C. Cir. 2019) (on a motion to dismiss "we assume the truth of all plaintiffs' plausibly pleaded allegations, and draw all reasonable inferences in their favor"). Notably, at least one named plaintiff purchased credit monitoring services *before* OPM's offered services were "up and running." *Compare* Hearing Tr. 35, *with* Arnold Plaintiffs' Compl. ¶ 28, J.A 48–49.

Second, seven of the named Arnold Plaintiffs had accounts opened and purchases made in their names. For example, Kelly Flynn and her husband had several new credit card accounts fraudulently opened in their names. They also discovered that two separate loans totaling $6,400 had been taken out in their names without their permission and were now delinquent. Those financial losses qualify as "actual damages." *See Cooper*, 566 U.S. at 298–299.

The district court deemed those damages insufficient because Arnold Plaintiffs did not further allege that their costs went unreimbursed. That was error. At this stage of the litigation, all facts and reasonable inferences must be drawn in favor of Arnold Plaintiffs, and the complaint provides no basis for disregarding the claimed financial losses based on OPM's speculation that Arnold Plaintiffs were indemnified. *See Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 513–514 (D.C. Cir. 2016).

Anyhow, "an injured person may usually recover in full from a wrongdoer regardless of anything he may get from a

collateral source unconnected with the wrongdoer." *Kassman v. American Univ.*, 546 F.2d 1029, 1034 (D.C. Cir. 1976) (per curiam) (formatting altered); *accord* Restatement (Second) of Torts § 920A(2). That rule prevents the victim's benefits from becoming the tortfeasor's windfall. *See Hudson v. Lazarus*, 217 F.2d 344, 346 (D.C. Cir. 1954). So too here.

OPM also objects that only some forms of reimbursement qualify for the collateral source rule. Gov't Br. 45. Again, OPM gets the cart before the horse, because the complaint contains no allegations about recompense at all, let alone what their sources were. OPM's argument also offers an overly cramped vision of the collateral source rule. *See Hudson*, 217 F.2d at 346 (without limiting the collateral source rule's application, observing that it applies to "gift[s] or the product of a contract of employment or of insurance"); Restatement (Second) of Torts § 920A cmt. c (offering a non-exclusive list of "types of benefits" to which the collateral source rule applies); *see also, e.g.*, *Temme v. Bemis Co.*, 762 F.3d 544, 549 (7th Cir. 2014) (per curiam) (applying the collateral source rule to attorneys' fees payments).

Third, Plaintiffs Kelly Flynn and six others had false tax returns filed using their information and have experienced delays in receiving federal and state tax refunds. The delay in those Plaintiffs' receipt of their refunds, and the forgone time value of that money, is an actual, tangible pecuniary injury.

OPM argues "no harm, no foul" because the Internal Revenue Service must pay taxpayers interest due for delayed refunds. *See* 26 U.S.C. § 6611. That misses the mark. To start, interest on tax overpayments is itself taxable income, *id.* § 61(a)(4); *Megibow v. Commissioner*, 102 T.C.M. (CCH) 232 (2011), while interest incurred in taking out loans to cover the delayed refunds is not deductible, 26 U.S.C. § 163(h)(1). That

makes the IRS's payment scheme inherently under compensatory. On top of that, the IRS pays interest only on delayed *federal* refunds, not state tax refunds. Arnold Plaintiffs' Compl. ¶ 28, J.A. 49 (alleging delay in state tax refund); *see generally* 26 U.S.C. § 6611(a) ("Interest shall be allowed and paid upon any overpayment in respect of any *internal revenue tax*.") (emphasis added).

Lastly, one Plaintiff, Lillian Gonzalez-Colon, spent more than 100 hours to resolve the fraudulent tax return filing and to close a fraudulently opened account. Those efforts "required her to take time off work[]" to address the consequences of the OPM breach. Arnold Plaintiffs' Compl. ¶ 31, J.A. 50–51; *see Beaven*, 622 F.3d at 557–559 (concluding that plaintiffs could claim damages for "lost time" spent "dealing with the disclosure" of their Bureau of Prison personnel files).

OPM urges us to hold Gonzalez-Colon to Federal Rule of Civil Procedure 9(g)'s requirement that "special damages" be "specifically stated." Fed. R. Civ. P. 9(g). We have not yet addressed whether Rule 9(g)'s heightened pleading standard applies to Privacy Act claims, and we have no occasion to do so here. Gonzalez-Colon's specific allegations about the time lost from work addressing the fraudulent tax return and Verizon Wireless account suffice either way. *See* 5A Charles A. Wright & Arthur R. Miller, Federal Practice & Procedure § 1311 (4th ed. 2019) ("[A]llegations of special damage will be deemed sufficient for the purpose of Rule 9(g) if they are definite enough to notify the opposing party and the court of the nature of the damages and enable the preparation of a responsive pleading.").

For all of those reasons, Arnold Plaintiffs have adequately alleged actual damages within the meaning of the Privacy Act.

2

The complaint also explains how Arnold Plaintiffs' actual damages were the "result of" OPM's Privacy Act violations. 5 U.S.C. § 552a(g)(4)(A).

To meet the Privacy Act's causation requirement, Arnold Plaintiffs must plausibly allege that the OPM hack was the "proximate cause" of their damages. *Dickson v. Office of Pers. Mgmt.*, 828 F.2d 32, 37 (D.C. Cir. 1987). That is, OPM's conduct must have been a "substantial factor" in the sequence of events leading to Arnold Plaintiffs' injuries, and those injuries must have been "reasonably foreseeable or anticipated as a natural consequence" of OPM's conduct. *Owens v. Republic of Sudan*, 864 F.3d 751, 794 (D.C. Cir. 2017). To be the proximate cause is not necessarily to be the sole cause. *See Hecht v. Pro-Football, Inc.*, 570 F.2d 982, 996 (D.C. Cir. 1977). OPM was the proximate cause of the harm befalling Arnold Plaintiffs so long as its conduct created a foreseeable risk of harm through the hackers' intervention. *See Staub v. Proctor Hosp.*, 562 U.S. 411, 420 (2011); Restatement (Second) of Torts § 442A.

The complaint alleges facts demonstrating proximate cause. Arnold Plaintiffs contend that OPM's failure to establish appropriate information security safeguards opened the door to the hackers, giving them ready access to a storehouse of personally identifiable and sensitive financial information. In particular, the complaint explains that OPM's failure to adopt basic protective measures "foreseeably heightened the risk of a successful intrusion into OPM's systems." Arnold Plaintiffs' Compl. ¶ 134, J.A. 74. And its decisions to disregard the Inspector General's repeated warnings and "not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to

access and loot OPM's systems for nearly a year without being detected." *Id.*; *see id.* ¶¶ 105–113, J.A. 70–71.

The proof is in the pudding: Numerous Arnold Plaintiffs suffered forms of identity theft accomplishable only with the type of information that OPM stored and the hackers accessed. That directly links the hack to the theft of the victims' private information, the pecuniary harms suffered, and the ongoing increased susceptibility to identity theft or financial injury. *See* Arnold Plaintiffs' Compl. ¶¶ 14, 17, 21–22, 24–26, 28–29, 31–32, 34, 39–41, 45, 49, J.A. 40–59; *Attias v. CareFirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017) (plaintiffs plausibly alleged risk of identity theft for Article III standing purposes based on the nature of the stolen data), *cert. denied*, 138 S. Ct. 981 (2018).[3] To argue, as OPM does, that the presumed occurrence of other data breaches defeats a causal connection as a matter of law at this early stage again wrongly construes inferences drawn from generic assertions about the general risk of data breaches in the government's favor. The law would embody quite a "perverse

[3] *See also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012) (plaintiffs plausibly alleged that data breach proximately caused their identity theft for purposes of Florida law by "alleg[ing] that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity"); *Stollenwerk v. Tri–West Health Care All.*, 254 F. App'x 664, 667 (9th Cir. 2007) (plaintiff established that data breach proximately caused identity theft for purposes of Arizona law where plaintiff provided his personal information to defendant, the identity fraud incidents began six weeks after defendant's systems were compromised, and plaintiff had not previously suffered from identity theft); *In re Community Health Sys., Inc.*, No. 15-CV-222-KOB, 2016 WL 4732630, at *25 (N.D. Ala. Sept. 12, 2016) (plaintiff plausibly alleged causal link between data breach and identity theft by "alleg[ing] misuse occurring subsequent to the breach that would be consistent with the type of data stolen").

incentive" were it to hold at this threshold stage of litigation that, "so long as enough data breaches take place," agencies "will never be found liable." *In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1318 (N.D. Ga. 2019) (formatting altered); *accord In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 988 (N.D. Cal. 2016).

In any event, OPM makes no claim that these particular plaintiffs have been subjected to hacks of equivalent breadth and depth, sweeping in such acutely sensitive personal information as Social Security numbers, fingerprints, and birth certificates.

In sum, Arnold Plaintiffs have adequately alleged (i) that OPM willfully chose not to establish basic and necessary information security safeguards in violation of Section 552a(e)(10) of the Privacy Act, and (ii) that those actions proximately caused (iii) actual damages in multiple, specific ways. Because the complaint, at this threshold stage, states a viable Privacy Act claim, OPM's sovereign immunity has been waived.

IV

In addition to their Privacy Act claim against OPM, Arnold Plaintiffs assert statutory and common law claims against OPM's contractor, KeyPoint Government Solutions. Arnold Plaintiffs' Compl. ¶¶ 208–275, J.A. 94–110 (alleging negligence, negligent misrepresentation and concealment, invasion of privacy, violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681, violation of "State Statutes Prohibiting Unfair and Deceptive Trade Practices," violation of "State Data Breach Acts," and breach of contract).

OPM tasked KeyPoint with performing background and security clearance investigations and inputting the sensitive information it collected into OPM's electronic recordkeeping system. The hackers allegedly were able to obtain KeyPoint credentials and then used them to gain access to OPM's network. *See* Arnold Plaintiffs' Compl. ¶ 106, J.A. 70.

The district court held that, as OPM's contractor, KeyPoint enjoyed "derivative sovereign immunity" from those claims. We review the applicability of derivative sovereign immunity *de novo*, *see Cunningham v. General Dynamics Info. Tech., Inc.*, 888 F.3d 640, 645 (4th Cir. 2018), *cert. denied*, 139 S. Ct. 417 (2018), and find no basis for its application in this case. OPM's contract obligated KeyPoint to meet the same standards for protecting personal information that the Privacy Act imposes directly on OPM. Because the improper conduct alleged would have violated the Privacy Act if committed by OPM itself and because KeyPoint's challenged misconduct was not directed by OPM, there is no sovereign immunity for KeyPoint to derive.[4]

As a private company, KeyPoint ordinarily would not enjoy immunity against the statutory and tort claims asserted by Arnold Plaintiffs. But government contractors may sometimes "obtain certain immunity in connection with work which they do pursuant to their contractual undertakings with the United States." *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672 (2016) (internal quotation marks omitted) (quoting *Brady v. Roosevelt S.S. Co.*, 317 U.S. 575, 583 (1943)).

[4] Neither OPM nor the Justice Department in its brief in this case has endorsed KeyPoint's claim of derivative sovereign immunity.

Derivative sovereign immunity, though, is less "embracive" than the immunity a sovereign enjoys. *Campbell-Ewald*, 136 S. Ct. at 672. It applies only when a contractor takes actions that are "authorized and directed by the Government of the United States," and "performed pursuant to the Act of Congress" authorizing the agency's activity. *Id.* at 673. In that way, derivative sovereign immunity ensures that "'there is no liability on the part of the contractor' who simply performed as the Government directed." *Id.* (quoting *Yearsley v. W.A. Ross Constr. Co.*, 309 U.S. 18, 21 (1940)); *id.* at 673 n.7 ("Critical in *Yearsley* was not the involvement of public works, but the contractor's performance in compliance with all federal directions."). Said another way, a government contractor that "violates both federal law and the government's explicit instructions" loses the shield of derivative immunity and is subject to suit by those adversely affected by the contractor's violations. *Id.* at 672.

Like the plaintiff in *Campbell-Ewald*, Arnold Plaintiffs have plausibly alleged that KeyPoint's failure to secure its credentials ran afoul of both OPM's explicit instructions and federal law standards, rendering derivative sovereign immunity unavailable.

At the outset, KeyPoint's failure to place in the record its contract with OPM makes it particularly difficult for it to establish, on a motion to dismiss, that its alleged security lapses were "authorized and directed" by OPM, *Campbell-Ewald*, 136 S. Ct. at 673 (quoting *Yearsley*, 309 U.S at 20). *See generally Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1133 (D.C. Cir. 2015).

In fact, Privacy Act regulations require OPM, when contracting "for the operation * * * of a system of records to accomplish an agency function," to "cause the requirements"

of the Privacy Act to be "applied to such system." 5 U.S.C. § 552a(m)(1); *see* 48 C.F.R. §§ 24.102(a), 24.104, 52.224-2. KeyPoint does not deny that. So KeyPoint was obligated by contract and regulation to, among other things, establish "appropriate safeguards to insure the security and confidentiality of records." 5 U.S.C. § 552a(e)(10); *see* Arnold Plaintiffs' Compl. ¶ 123, J.A. 72–73.

The complaint expressly asserts that KeyPoint failed to fulfill those obligations, which led to the break-in. KeyPoint allegedly violated its regulatory and contractual obligations, among other things, to (i) "secure its systems for gathering and storing" government investigation information despite "knowing of [its] vulnerabilities;" (ii) "comply with industry-standard data security practices;" (iii) "perform requisite due diligence and supervision in expanding its workforce;" (iv) "encrypt [government investigation information] at collection, at rest, and in transit;" (v) "employ adequate network segmentation and layering;" (vi) "ensure continuous system and event monitoring and recording;" and (vii) "otherwise implement security policies and practices sufficient to protect * * * [government investigation information] from unauthorized disclosure." Arnold Plaintiffs' Compl. ¶ 223, J.A. 98. Notably, it was KeyPoint's alleged failure to secure and protect its employees' log-in credentials that allowed the hackers to access OPM's system in May 2014, and it was from there that the hackers ultimately stole 21.5 million background investigation records.

Unsurprisingly, KeyPoint does not argue that OPM "authorized and directed" it to design its system with the security flaws that Arnold Plaintiffs identify. *Campbell-Ewald*, 136 S. Ct. at 673. So KeyPoint cannot wrap itself in derivative immunity garb on the ground that it "simply performed as the Government directed." *Id.*

The district court felt differently, concluding that derivative immunity applied because the Privacy Act is wholly inapplicable to KeyPoint. It is true that the Privacy Act itself does not apply directly to government contractors like KeyPoint. *See Abdelfattah v. Department of Homeland Security*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) ("[T]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individual officials.").

But that is beside the point. To claim immunity, KeyPoint had to establish "compliance with all federal directions" pertaining to its relevant conduct, including the regulatory and contractual obligation to meet the Privacy Act's standards in its contract operations. *Campbell-Ewald*, 136 S. Ct. at 673 n.7.

So what matters for derivative sovereign immunity purposes is KeyPoint's (i) inability to point to a contractual provision or other OPM direction authorizing or directing the very gaps in security protections over which Arnold Plaintiffs are suing, and (ii) its *regulatory* duty to ensure informational security equivalent to that demanded by the Privacy Act. 48 C.F.R. §§ 24.102(a), 24.104, 52.224-2. Add to that the absence of sovereign immunity protections for OPM from the Privacy Act claims in this case, and the sovereign immunity well from which KeyPoint seeks to draw has run dry.

The district court also pointed to Section 552a(m)(1) of the Privacy Act, which provides that the contractor and its employees "shall be considered employees of the agency[,]" and to a regulation providing that "the system of records operated under the contract is deemed to be maintained by the agency." *In re OPM*, 266 F. Supp. 3d at 48–49 (quoting 48

C.F.R. § 24.102(c)). Neither supports the application of derivative sovereign immunity here.

Even under the district court's reading, Section 552a(m)(1) hurts rather than helps KeyPoint. OPM's and its employees' own immunity has been waived. So treating KeyPoint employees like OPM employees gets KeyPoint nowhere. It cannot derive an immunity that OPM itself does not have. *See Campbell-Ewald*, 136 S. Ct. at 666 (asking whether "*the sovereign's* immunity from suit shield[s] the [contractor] * * * as well") (emphasis added); *see also Contango Operators, Inc. v. United States*, 965 F. Supp. 2d 791, 814 (S.D. Tex. 2013) (because "[n]o sovereign immunity has been established," the court "therefore concludes that there is no governmental immunity from which an immunity may be derived for the benefit of" the contractor), *aff'd sub nom. Contango Operators, Inc. v. Weeks Marine, Inc.*, 613 F. App'x 281 (5th Cir. 2015); *cf. McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1345 (11th Cir. 2007) (reasoning that if a federal officer cannot claim complete derivative immunity, then neither can a mere common law agent, because otherwise "a prison guard employed by the government would have only qualified immunity, while a private contractor who works in the prison but is no more than a common law agent would have absolute immunity").

After all, the driving purpose of derivative sovereign immunity "is to prevent the contractor from being held liable when the government is actually at fault but is otherwise immune from liability." *In re World Trade Center Disaster Site Litig.*, 456 F. Supp. 2d 520, 560 (S.D.N.Y. 2006) (internal quotation marks omitted), *aff'd*, 521 F.3d 169 (2d Cir. 2008); *cf. Filarsky v. Delia*, 566 U.S. 377, 390–391 (2012) (if qualified immunity is withheld from private individuals "acting on behalf of the government," "government employees will

often be protected from suit by some form of immunity, [while] those working alongside them could be left holding the bag—facing full liability for actions taken in conjunction with government employees who enjoy immunity for the same activity").

In any event, the district court overread the statute. When the Privacy Act speaks of contractors as "employees" of the agency, it does so for the purpose of extending *criminal* liability to contractors and their employees if they violate certain Privacy Act requirements. 5 U.S.C. § 552a(i), (m)(1). Congress's decision to subject federal contractors to the same Privacy Act criminal prohibitions as their agency employers hardly augurs in favor of according those same contractors *more* protection from civil liability than the agency itself.

As for the district court's reliance on 48 C.F.R. § 24.102(c), that regulation says nothing about contractors' responsibility for complying with their contractual and regulatory obligations. The rule simply holds the contracting agency responsible for "the system of records operated under the contract." 48 C.F.R. § 24.102(c), (d). Which makes sense. Otherwise, the government would be able to contract itself out of the Privacy Act obligations that Congress imposed.

Beyond that, KeyPoint's argument frequently mixes apples and oranges, citing preemption cases in an effort to substantiate its claim to derivative immunity. KeyPoint Br. 24–26. That tactic will not work. Those preemption cases do not turn on the applicability of derivative sovereign immunity. And KeyPoint has not raised a preemption argument in this court, so any argument to that effect is forfeited for purposes of this appeal. *See Al-Tamimi v. Adelson*, 916 F.3d 1, 6 (D.C. Cir. 2019) ("A party forfeits an argument by failing to raise it in his opening brief.").

In sum, derivative sovereign immunity has its limits. KeyPoint exceeded those limits, and for that reason cannot don the cloak of derivative sovereign immunity.

V

Finally, we turn to NTEU Plaintiffs' constitutional claim. In that claim, NTEU Plaintiffs do not allege that OPM intentionally disclosed the records at issue or performed the functional equivalent of such a disclosure. *See, e.g.*, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186 (alleging "reckless indifference"). Instead, NTEU Plaintiffs challenge OPM's internal record-management and storage practices and policies as unconstitutionally trenching on their asserted constitutional right to privacy. *See, e.g.*, *id.* at 3, J.A. 155 ("Although on notice of serious flaws in its data system security, OPM failed to adequately secure personal information in its possession—a failure that was reckless under the circumstances."). They appear to rely on two closely related threads of constitutional doctrine, one couched in terms of privacy and relying mainly on dicta from *Whalen v. Roe*, 429 U.S. 589 (1977), the other phrased more directly in terms of substantive due process and relying mainly on cases providing relief for persons harmed through government neglect of their personal safety. We address them in that order.

A

As NTEU Plaintiffs see it, the Constitution creates a "zone of privacy" that protects an individual's "interest in avoiding disclosure of personal matters." NTEU Br. 36 (quoting *Whalen*, 429 U.S. at 598–599). This putative right to "informational privacy," they contend, is violated not only where government agents intentionally disclose an individual's

personal information, but where, as alleged here, the agents "reckless[ly]" fail to prevent a third party from stealing it. NTEU Plaintiffs' Compl. 3, J.A. 155; *see also* Oral Arg. Tr. 44:23–45:5.

Even assuming "without deciding[] that the Constitution protects" some "sort" of privacy "interest in avoiding disclosure of personal matters," *NASA v. Nelson*, 562 U.S. 134, 138 (2011) (quoting *Whalen*, 429 U.S. at 599–600), NTEU Plaintiffs have failed to state a legally cognizable claim. There is no authority for their contention that the Constitution imposes on the government an affirmative duty—untethered to specific constitutional provisions such as the First Amendment, *see, e.g.*, *Americans for Prosperity Found. v. Becerra*, 903 F.3d 1000, 1019 (9th Cir. 2018)—to "safeguard personal information" from the criminal acts of third parties, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186.

The asserted duty to "adequately secure" government computer networks finds no support in the Constitution or our history. NTEU Plaintiffs' Compl. 3, J.A. 155. Not once do NTEU Plaintiffs quote the very document from which they purport to derive their claimed right: the Constitution of the United States. Nor, for that matter, do they invoke this "Nation's history and tradition," *Aka v. United States Tax Court*, 854 F.3d 30, 34 (D.C. Cir. 2017) (quoting *Washington v. Glucksberg*, 521 U.S. 702, 720–721 (1997))—an integral part of the formula for identifying *unenumerated* rights.

NTEU Plaintiffs instead ground their claim in a single line of Supreme Court dictum from more than 40 years ago that describes "[t]he cases sometimes characterized as protecting 'privacy'" as involving, among other interests, a vague "individual interest in avoiding disclosure of personal matters." NTEU Br. 36 (quoting *Whalen*, 429 U.S. at 599). But neither

we nor the Supreme Court has ever held that this interest is a constitutional right. *American Fed'n of Gov't Employees v. Department of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997) ("The Supreme Court has addressed the issue in recurring dicta without, we believe, resolving it."). Both courts have, so far, steadfastly rejected all informational privacy claims purporting to rest on the Constitution, while simply "assum[ing]"—but never "deciding"—that the Constitution protects a "right of the sort mentioned in *Whalen*." *NASA*, 562 U.S. at 138; *see Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457–458 (1977); *Whalen*, 429 U.S. at 605; *American Fed'n of Gov't Employees*, 118 F.3d at 791. Indeed, neither this court nor the Supreme Court has ever elaborated on the rationale for—or even defined the "precise contours of"—the putative right to informational privacy. *American Fed'n of Gov't Employees*, 118 F.3d at 793; *see also, e.g.*, *NASA*, 562 U.S. at 147–148. Rather, we have underlined its "ambiguity." *National Fed'n of Fed. Employees v. Greenberg*, 983 F.2d 286, 293 (D.C. Cir. 1993); *cf. Siegert v. Gilley*, 500 U.S. 226, 233–234 (1991) (holding that even malicious government defamation does not trigger constitutional protection) (citing *Paul v. Davis*, 424 U.S. 693 (1976)).

Other circuits, to be sure, have embraced a form of the putative right. *See, e.g.*, *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999); *see also NASA*, 562 U.S. at 146 n.9 (collecting cases). *But see Doe v. Wigginton*, 21 F.3d 733, 740 (6th Cir. 1994). But NTEU Plaintiffs have identified no case in which the government has been held to have violated the alleged right without having "*affirmatively provid[ed]* the protected information to those unauthorized to view it." NTEU Br. 47 (emphasis added). Neither have we. Absent any plausible mooring in the Constitution's text or the Nation's history and tradition, we join the district court in declining to recognize the proposed constitutional right to informational privacy that

would be violated not only when information is intentionally disclosed (or the functional equivalent), but also "when a third party *steals* it." *In re OPM*, 266 F. Supp. 3d at 46.

Troubled as we are by NTEU Plaintiffs' allegations regarding the severity and scope of OPM's data security shortcomings, we are nonetheless reluctant to constitutionalize an information security code for the government's "internal operations." *NASA*, 562 U.S. at 151 (citing *Engquist v. Oregon Dep't of Agric.*, 553 U.S. 591, 598–599 (2008)). OPM "collect[ed] and store[d]" the information at issue here not as sovereign, but as employer—in "its role as the federal civil service's personnel manager." NTEU Plaintiffs' Compl. ¶ 10, J.A. 159. In this capacity—"'as proprietor' and manager of [the government's] 'internal operation,'" *NASA*, 562 U.S. at 148 (quoting *Cafeteria & Rest. Workers Union v. McElroy*, 367 U.S. 886, 896 (1961))—OPM was "dealing 'with citizen *employees*,'" and thus had a "much freer hand" than it would have had if it had brought "its sovereign power to bear on citizens at large," *id.* (emphasis added) (quoting *Engquist*, 553 U.S. at 598). That "freer hand" exists for good reason. Whereas the "Constitution requires that a President chosen by the entire Nation oversee the execution of the laws," albeit by a "vast and varied federal bureaucracy," *Free Enter. Fund v. Public Co. Accounting Oversight Bd.*, 561 U.S. 477, 499 (2010), constitutionally micromanaging employment records management systems, reaching down to the details of "how [best] to protect" the "information systems" holding employee data, NTEU Br. 48, would shift a material part of that oversight function to the judiciary, which generally lacks established standards or guideposts for making such administrative judgments—at least in the absence of congressional direction. *Cf. Bishop v. Wood*, 426 U.S. 341, 349–350 (1976).

Another reason counsels hesitation. Establishing judicial supervision over the security of the government's employee data would "short-circuit" the response that Congress has already launched. *District Attorney's Office for Third Judicial Dist. v. Osborne*, 557 U.S. 52, 73 (2009) (citing *Glucksberg*, 521 U.S. at 720). As the Supreme Court observed in *NASA*, Congress has in the Privacy Act adopted significant "protections against disclosure" of personal information that "'evidence a proper concern' for individual privacy." 562 U.S. at 156 (quoting *Whalen*, 429 U.S. at 605). Here, as there, the Act limits the government's ability to maintain records "about an individual," 5 U.S.C. § 552a(e)(1), and "imposes criminal liability for willful violations of its nondisclosure obligations," 562 U.S. at 156 (citing 5 U.S.C. § 552a(i)(1)). NTEU Plaintiffs, of course, allege that OPM has "fail[ed] to satisfy" these obligations, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186, and argue that their "inherently personal information remains at substantial risk of additional breaches because" of OPM's failures, Oral Arg. Tr. 49:17–19. But if NTEU Plaintiffs are right (as we must assume in the current posture of the case), then they may invoke the remedial provisions found by Congress to best balance privacy and competing interests. *See* 5 U.S.C. § 552a(g)(1)(D), (g)(4); *cf. supra* Part III.A (reversing dismissal of Arnold Plaintiffs' Privacy Act claims).

Establishing a freestanding constitutional right to informational privacy that creates a duty to safeguard personal information from unauthorized access by third parties would force us to develop a labyrinth of technical rules. *See Osborne,* 557 U.S. at 73–74. For example, does the Constitution require data "encrypt[ion]"? NTEU Br. 6 (citing NTEU Plaintiffs' Compl. ¶¶ 51–52, J.A. 172–173). If so, must all data be encrypted in transit, as well as at rest? *Cf.* Arnold Plaintiffs' Compl. ¶¶ 136, 223, J.A. 75, 98. What of the encryption key: Is 256 bits necessary—or would 128 bits scrape by,

constitutionally speaking? *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 993 (2018) (illustrating the difference). How about "personal identity verification (PIV) credentials"—are they constitutionally mandated? NTEU Plaintiffs' Compl. ¶ 47, J.A. 171 (internal quotation marks omitted). And most significant: What "tools" should "federal courts * * * use to answer" these questions? *Osborne*, 557 U.S. at 74. NTEU Plaintiffs do not say; more important, neither does the Constitution.

We therefore hold that, assuming (without deciding) the existence of a constitutional right to informational privacy, *see, e.g.*, *NASA*, 562 U.S. at 138; *American Fed'n of Gov't Employees*, 118 F.3d at 791, it affords relief only for intentional disclosures or their functional equivalent—which NTEU Plaintiffs do not allege.

B

NTEU Plaintiffs also seek to ground their claim in the Due Process Clause of the Fifth Amendment, contending specifically that, in some instances, "reckless or deliberate indifference" (as opposed to intentional misconduct) "may 'shock the conscience sufficiently to violate due process.'" NTEU Reply Br. 13 (quoting *Smith v. District of Columbia*, 413 F.3d 86, 93 (D.C. Cir. 2005)); *see also* NTEU Br. 47–48; Oral Arg. Tr. 74:3–9. True enough. *See, e.g.*, *United States v. Salerno*, 481 U.S. 739, 746 (1987) (citing *Rochin v. California*, 342 U.S. 165, 172 (1952)).

But the conscience's susceptibility to shock varies radically with whether the government has previously taken an "affirmative act of restraining the individual's freedom to act on his own behalf—through incarceration, institutionalization, or similar restraint of personal liberty." *DeShaney v. Winnebago Cnty. Dep't of Soc. Servs.*, 489 U.S. 189, 200

(1989). Thus, a prisoner who has "already been deprived of [his] liberty," for example, has a plausible claim to affirmative governmental protection. *Collins v. City of Harker Heights*, 503 U.S. 115, 127 (1992); *see also Smith*, 413 F.3d at 94–95 (same for "juvenile delinquent held 'against his will'"). Absent such a restraint, however, the government's "failure to protect an individual from private [acts], even in the face of known danger, [generally] 'does not constitute a violation of the Due Process Clause.'" *Butera v. District of Columbia*, 235 F.3d 637, 647 (D.C. Cir. 2001) (quoting *DeShaney*, 489 U.S. at 197). "The state must protect those it throws into snake pits, but the state need not guarantee that volunteer snake charmers will not be bitten." *Walker v. Rowe*, 791 F.2d 507, 511 (7th Cir. 1986) (explaining that although a state has a constitutional duty to protect prisoners in its custody, it has no such obligation toward prison guards who have voluntarily accepted employment with the state).

Here, NTEU Plaintiffs' claims fall on the wrong side of this line; they assert an affirmative government duty to safeguard personal information that current and prospective employees *voluntarily* submitted to the government.

This lack of compulsion makes all the difference. In *Collins*, for example, the Supreme Court rejected the claim—made by the widow of a city sanitation worker killed in the performance of his duties—that the Due Process Clause required the government to "provide its employees with certain minimal levels of safety and security." 503 U.S. at 127. A government employee, the Court reasoned, could not maintain "that the [government] deprived [him] of his liberty"—and thus incurred a "continuing obligation" to protect that liberty by guaranteeing him a minimum level of safety and security—"when it made, and he voluntarily accepted, an offer of employment." *Id.* at 128. That is precisely why, applying the

principle in cases posing the distinction most directly, we have rejected claims by prison guards. *See Fraternal Order of Police Dep't of Corrs. Labor Comm. v. Williams*, 375 F.3d 1141, 1147 (D.C. Cir. 2004); *Washington v. District of Columbia*, 802 F.2d 1478, 1482 (D.C. Cir. 1986).

Similar logic applies here. Like the sanitation worker in *Collins*—and the prison guards in *Williams* and *Washington*—NTEU Plaintiffs "voluntarily" sought and "accepted" an "offer of [government] employment." *Collins*, 503 U.S. at 128. In doing so, they voluntarily submitted personal information "as part of a background investigation." NTEU Plaintiffs' Compl. ¶ 60, J.A. 176. In no sense, then, did the government compel NTEU Plaintiffs to seek government employment; it therefore bore no constitutional duty under the Due Process Clause to protect them from the risks associated with applying for such positions. With no triggering deprivation of liberty or property to speak of, there arose no constitutional governmental duty to "provide [NTEU Plaintiffs] with certain minimal levels of safety and security," *Collins*, 503 U.S. at 127—physical or digital.

VI

In sum, we reverse in part and affirm in part. We hold that (i) NTEU and Arnold Plaintiffs have adequately alleged Article III standing; (ii) Arnold Plaintiffs have stated a claim under the Privacy Act, which waives OPM's sovereign immunity; (iii) KeyPoint is not protected by derivative sovereign immunity; and (iv) NTEU Plaintiffs have failed to state a claim that flaws in OPM's information-storage measures violated the Constitution. We remand for further proceedings consistent with this opinion.

So ordered.

WILLIAMS, *Senior Circuit Judge*, concurring in part and dissenting in part:

Why did "sophisticated" cyberintruders spend several months systematically and covertly extracting 21.5 million highly sensitive background investigation records for federal government employees from the Office of Personnel Management? Arnold Plaintiffs' Compl. ¶ 128, J.A. 73. Plaintiffs' answer is identity theft. Might the hackers have been members of a criminal syndicate looking to sell the information to identity thieves on the dark web to bilk victims such as Mr. Travis Arnold out of "approximately $125"? *Id.* ¶ 13, J.A. 40. Yes, theoretically. But as a basis for standing for most Arnold Plaintiffs the garden-variety identity theft theory lacks the necessary plausibility in light of an obvious alternative explanation: The breach "d[oes] not plausibly suggest" identity theft as the motive (and hence a source of future harm) because it is "more likely explained" as the handiwork of foreign spies looking to harvest information about millions of federal workers for espionage or kindred purposes having nothing to do with identity theft. *Ashcroft v. Iqbal*, 556 U.S. 662, 680 (2009); see Br. of Chamber of Commerce of U.S. as *Amicus Curiae* in Support of Appellees 6 ("Nation-states frequently target personally identifying information . . . in order to spy on certain individuals." (brackets omitted)).

My colleagues do not deny the possibility. See *Maj. op.* 17 ("[A] cyberattack on a government system might well be motivated by a purpose other than identity theft . . . ."). Yet, in assessing standing, they conclude that "all" 21.5 million Arnold Plaintiffs have "plausibly alleged a substantial risk" that they will, due to this particular data breach, suffer "future identity theft." *Id.* at 14, 25.

Respectfully, I disagree. Because Arnold Plaintiffs have failed to allege facts that would tend to negate the "obvious

alternative explanation" for the breach (i.e., espionage), they have not, in my view, "nudged [their] claims . . . across the line from conceivable to plausible." *Iqbal*, 556 U.S. at 680, 682 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 567, 570 (2007)). I would therefore affirm the dismissal of Arnold Plaintiffs' claims for lack of standing—with one exception, discussed below. As a result, I join the court's opinion in full except with respect to any portions that are inconsistent with this dissent, including but not limited to Parts II.B (holding that Arnold Plaintiffs stated a plausible claim to standing) and III.B.2 (holding that Arnold Plaintiffs stated a plausible claim that their injuries were the "result of" the breach).

* * *

Two aspects of the standing analysis are important here. First, standing "depends on the facts as they exist[ed] when the complaint [was] filed." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 569 n.4 (1992) (emphasis removed) (quoting *Newman-Green, Inc. v. Alfonzo-Larrain*, 490 U.S. 826, 830 (1989)). We therefore look, not to the apparent risk of future identity theft in, say, May *2014*—the date of the first major breach, see Arnold Plaintiffs' Compl. ¶ 127, J.A. 73—but to the risk apparent in March *2016*, when Arnold Plaintiffs filed their operative complaint.

Second, standing "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Lujan*, 504 U.S. at 561). Thus, "at the motion to dismiss stage," Arnold Plaintiffs' standing allegations must satisfy the pleading requirements of *Twombly* and *Iqbal*—that is, the complaint must state "'a plausible claim' that each element of standing is

satisfied." *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 513 (D.C. Cir. 2016) (quoting *Iqbal*, 556 U.S. at 678–79). This standard "asks for more than a sheer possibility," *Iqbal*, 556 U.S. at 678, that Arnold Plaintiffs faced a "substantial risk" that future injury would occur, *Susan B. Anthony List*, 573 U.S. at 158 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). Facts "that are 'merely consistent with'" a substantial risk of future identity theft fall "'short of the line between possibility and plausibility of 'entitlement to relief.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557).

Under these standards, most Arnold Plaintiffs lack standing. This is not your typical case, where hackers break into a commercial entity's servers and steal consumer information. In those cases, it is generally fair to infer—as this court has inferred—that the hackers plan to, "sooner or later," "make fraudulent charges or assume [the victims'] identities." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628–29 (D.C. Cir. 2017) (quoting *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015)). "Why else would hackers break into a . . . database and steal consumers' private information?" *Id*. at 628 (alteration in original) (quoting *Remijas*, 794 F.3d 693). In such cases there's no obvious alternative explanation.

But here there is. In this case, hackers infiltrated a *government* system and stole sensitive "government investigation information," Arnold Plaintiffs' Compl. ¶ 1, J.A. 36, about *government* employees shortly after a cyberattack on the same agency had "compromised critical security documents," *id*. ¶ 3, J.A. 37. It is thus fair to infer, as the majority quite rightly recognizes, that the hackers "might well [have been] motivated by a purpose other than identity theft," *Maj. op.* 17, such as obtaining secret information from the persons in the files by extortion or surveillance, enlisting them as agents, obtaining leverage over American businesses, or

otherwise jeopardizing U.S. national security, see Br. of Chamber of Commerce of U.S. as *Amicus Curiae* in Support of Appellees 6; cf. Arnold Plaintiffs' Compl. ¶ 1, J.A. 36 (explaining that exposed and stolen information includes "private facts collected in federal background and security clearance investigations"); see also *id.* ¶ 129, J.A. 73–74 (specifying that the theft covered "many million questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information"). This espionage motive is, as *Iqbal* and *Twombly* put it, an "obvious alternative explanation"—an explanation that Arnold Plaintiffs, to survive a motion to dismiss, must deflect. *Iqbal*, 556 U.S. at 682 (quoting *Twombly*, 550 U.S. at 567).

This they fail to do. Just as "parallel conduct" in *Twombly* "does not suggest conspiracy" in antitrust cases because it is consistent with "independent action" in competitive markets, *Twombly*, 550 U.S. at 556–57; and just as detention of "thousands of Arab Muslim men" in *Iqbal* does not suggest discrimination because (given the identity of the September 11th attackers) it is consistent with legitimate law enforcement activity, *Iqbal*, 556 U.S. at 681–82, so too a "cyberattack on a government system" does not suggest identity theft (of the type alleged by plaintiffs) because it is consistent with an obvious alternative explanation—foreign espionage, *Maj. op.* 17; see also *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (finding no standing based on a "risk of future identity theft" where there is no evidence that the thief stole the laptop "with the intent to steal [plaintiffs'] private information").

What of dual motives, asks the majority? Couldn't the hackers have been interested in espionage *and* identity theft? *Maj. op.* 18. Yes, that's *conceivable*. But does the conceivability actually render plaintiffs' theory plausible? I don't think so. The majority invokes a syllogism: Because

"espionage and identity theft are not mutually exclusive," it follows that ascribing an "espionage-related motive" doesn't "render[] implausible" an allegation of "future risk of identity theft and financial fraud" caused by the data breach. *Id.* But it does exactly that. To begin with, even if the alternative explanations in *Iqbal* and *Twombly* happened to be mutually exclusive with plaintiffs' theories, the Court has never suggested that mutual exclusivity is a *prerequisite* to one plausible explanation's rendering some other explanation implausible. This case shows why such a prerequisite would be overkill. Just because two states of affairs *can* co-occur doesn't make their co-occurrence *plausible*—the legal standard plaintiffs must clear—nor does an otherwise implausible theory get bootstrapped into a plausible one merely because it's conceivable that it could co-occur with an obvious alternative explanation.

So while a foreign government might theoretically have enlisted "sophisticated" hackers to execute a "massive" cyberattack on the U.S. government over the course of "several months" to steal highly "sensitive" information, *Maj. op.* at 21, both to (i) compromise U.S. national security *and* (ii) commit fraud by (for example) purchases through an unauthorized Best Buy account (Arnold Plaintiffs' Compl. ¶ 39, J.A. 54), this dual-motive hypothesis seems fanciful for at least two reasons. First, the goal of identity theft is financial gain. The notion that a foreign state pursuing a complex, risky, and possibly expensive cyberespionage scheme would have as even one of its goals the extraction of small-potatoes sums from individuals by, e.g., filing fraudulent returns with the *United States* IRS or creating a "My Social Security" account, see *id.* ¶ 14, J.A. 40–41, falls far short of plausibility. Second, and more important, a foreign power seeking leverage over the United States would be most unlikely to permit its agents to use or sell the data for identity theft purposes, as doing so would risk *sabotaging* the

espionage goal. If data gleaned from the hack is slated for counterintelligence use, identity theft would undercut this aim by alerting victims and causing them to alter their data. Since the expected value of successful counterintelligence likely far exceeds that of identity theft, an espionage explanation affirmatively suggests that identity theft *will not* co-occur. And that is precisely what the record suggests. There is, as discussed below, a striking dearth of allegations as to any pattern of unusual or higher-than-ordinary identity theft or fraud among Arnold Plaintiffs. What readily comes to mind is an obvious alternative explanation—hacking focused entirely on pursuit of espionage and kindred threats to national security.

Thus the Sixth Circuit's caution—that "[f]erreting out the most likely reason for the defendants' actions is not appropriate at the pleadings stage," *Watson Carpet & Floor Covering, Inc. v. Mohawk Industries, Inc.*, 648 F.3d 452, 458 (6th Cir. 2011)—is inapt here. The court states in the immediately preceding sentence: "Often, defendants' conduct has several *plausible* explanations." *Id*. (emphasis added). Sorting out which among them is "most likely" is, indeed, out of bounds at the pleadings stage. Yet the whole thrust of my argument is that we haven't got "several plausible explanations." We have one alleged theory—identity theft—that, I argue, is not plausible in view of an obvious alternative explanation of far greater probability. Though it's unimpeachable logic to say that "[t]he plausibility of [one particular] reason for the refusals to sell carpet does not render all other reasons implausible," *id*., the point—made in context of a discussion of "several plausible explanations"—is not at play here, and marshaling it only begs the question whether identity theft is, in fact, a plausible explanation.

More is needed to "nudge[]" Arnold Plaintiffs' identity theft claims "across the line from conceivable to plausible."

Iqbal, 556 U.S. at 680 (quoting *Twombly*, 550 U.S. at 570). That is especially true here given the passage of time. As the initial breach occurred nearly *two years* before Arnold Plaintiffs filed their operative complaint, one would expect to see—if plaintiffs were right about the hackers' motives—some allegation linking Arnold Plaintiffs as a whole to the breach—such as indications that persons in the OPM databases suffered a relatively high rate of identity thefts, or a pattern of *similar* thefts. But there are no such allegations. And "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016)).

The majority generally agrees, conceding that the "passage of two years in a run-of-the-mill data breach might, absent allegation of subsequent data misuse, suggest that a claim of future injury is less than plausible." *Maj. op.* 21. Yet my colleagues think such an inference is not fair game here, where the breach occurred on "a massive scale" reflecting "a relatively new phenomenon." *Id*. Large-scale hacking is no doubt a recent phenomenon. But I can think of no attributes of such phenomena or their possible novelty that would invalidate a common sense expectation that future identity-theft-type injuries will become less plausible as time drags on without result. Whatever else may be true, if identity theft is an operative motive, time remains of the essence, given that much personal data—credit card numbers, bank account information, addresses—can go stale with time. If anything, the special features of this case make the passage of time exceptionally forceful in undermining plaintiffs' theory. The extraordinary volume of people affected and the exceptional sensitivity and range of the information captured should make it relatively easy to discern a "pattern of identity theft or financial fraud" among the pool of 21.5 million potential victims (and

litigants)—if there is one. *Id*. And yet, as the majority agrees, we have no "clearly identifiable pattern of identity theft or financial fraud" in the Complaint. *Id*.

To be sure, "certain Arnold Plaintiffs have already had fraudulent accounts opened and tax returns filed in their names." *Maj. op.* 19. But that is hardly probative. "In a society where around 3.3% of the population will experience some form of identity theft" in a given year, it is "not surprising" that a few plaintiffs in a putative class of 21.5 million would "have experienced some form of credit or bank-account fraud." *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1, 38 (D.D.C. 2017) (quoting *In re Science Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 32 (D.D.C. 2014)). A handful of Arnold Plaintiffs, for instance, almost certainly experienced a home invasion since the data breach. But that doesn't imply a "substantial risk" that *these hackers* have plans to break into the homes of garden-variety government employees.

In sum, Arnold Plaintiffs have alleged no facts—disproportionate incidence of identity theft, a distinctive pattern of fraud, or anything else of that sort among the putative class—that can credibly nudge their theory into the realm of plausibility in the face of an obvious alternative explanation. So they cannot "all" meet the threshold requirement for standing under the pleading standards of *Iqbal* and *Twombly*. *Maj. op.* 14.

I grant, of course, that in the immediate aftermath of the cyber-intrusion, some putative class members might reasonably have been unwilling to assume that the attack was motivated by a purpose other than identity theft. Thus, individuals at that early time, before the paucity of identity theft data emerged, might have "reasonably spent money to

protect themselves" from identity theft and thus have a plausible claim to standing to recover their expenses. *Attias*, 865 F.3d at 629. But that says nothing about whether, when plaintiffs filed their operative complaint two years later, all 21.5 million putative class members could *still* "reasonably" fear "a substantial risk" of identity theft. *Id*. at 629. They have shown no such thing.

* * *

For the subset of Arnold Plaintiffs who, as I see it, have standing, I turn to the issue of sovereign immunity. Arnold Plaintiffs file a battery of state law claims against a contractor that OPM engaged to perform background checks of prospective federal employees. That contractor, KeyPoint Government Solutions, Inc., maintains that, as a government contractor, it is entitled to sovereign immunity. The court, however, disagrees, see *Maj. op.* Part IV—and I join that part of the opinion in full.

I write separately to address an important distinction between contractor immunity, which KeyPoint asserts, and federal preemption, which KeyPoint fails to raise, and about which the court therefore expresses no views. See, e.g., KeyPoint's Br. 25 (distinguishing between preemption and immunity); Oral Arg. Tr. 31:3–21 (same); see also *Cunningham v. Gen. Dynamics Info. Tech., Inc.*, 888 F.3d 640, 646 n.4 (4th Cir. 2018) (same); *In re KBR, Inc., Burn Pit Litig.*, 744 F.3d 326, 342 n.6 (4th Cir. 2014) (same). Contractor immunity, it seems to me, immunizes only those acts that agents of the government are expressly directed by the government to perform—such as building a particular dike as "directed by the Government of the United States." See, e.g., *Yearsley v. W.A. Ross Construction Co.*, 309 U.S. 18, 20 (1940). Preemption, in contrast, is broader, knocking aside

state tort law to the extent that it impermissibly interferes with a contractor's ability to perform its federal obligations.

As the Supreme Court explained in *Boyle v. United Technologies Corp.*, there are "a few areas, involving 'uniquely federal interests,'" that "are so committed by the Constitution and laws of the United States to federal control that state law is pre-empted and replaced, where necessary, by federal law." 487 U.S. 500, 504 (1988) (quoting *Texas Industries, Inc. v. Radcliff Materials, Inc.*, 451 U.S. 630, 640 (1981)). The "civil liabilities arising out of the performance of federal procurement contracts" is one of them. *Id*. at 505–06. That is because "the Federal Government's interest in the procurement of equipment is implicated by" state tort suits, even where, as here, "the dispute is one between private parties." *Id*. at 506. Specifically, the "imposition of liability on Government contractors will directly affect the terms of Government contracts: either the contractor will decline to manufacture the design specified by the Government, or it will raise its price. Either way, the interests of the United States will be directly affected." *Id*. at 507.

To protect these interests, state law may be "displace[d]." *Id*. at 507. This will occur only where "a 'significant conflict' exists between an identifiable 'federal policy or interest and the [operation] of state law,'" *id*. (alteration in original) (quoting *Wallis v. Pan Am. Petroleum Corp.*, 384 U.S. 63, 68 (1966)), "or the application of state law would 'frustrate specific objectives' of federal legislation," *id*. (quoting *United States v. Kimbell Foods, Inc.*, 440 U.S. 715, 728 (1979)). "In some cases, for example where the federal interest requires a uniform rule, the entire body of state law applicable to the area conflicts and is replaced by federal rules." *Id*. at 508 (citing *Clearfield Trust Co. v. United States*, 318 U.S. 363, 366–67 (1943)). "In others, the conflict is more narrow, and only particular

elements of state law are superseded." *Id*. (citing *United States v. Little Lake Misere Land Co.*, 412 U.S. 580, 595 (1973)).

Here, there is a plausible argument for preemption. This case involves a fundamental federal issue—the hiring, vetting, and protecting of federal employees, and the balancing of the costs of keeping the relevant data secure against the costs of error or neglect in providing that security. And Congress, it seems, has already created a detailed statutory scheme in the form of the Privacy Act to address these (and other) issues. See, e.g., 5 U.S.C. § 552a(e)(10) (requiring "appropriate . . . technical . . . safeguards"). Under that scheme, the agency must, by contract, "cause the requirements of [the Privacy Act] to be applied" to the contractor's "system of records," see 5 U.S.C. § 552a(m)(1)—and if the *agency* fails to do so, then it faces potential liability, see *id*. § 552a(g)(1)(D); see also 48 C.F.R. § 24.102(d) ("Agencies, which within the limits of their authorities, fail to require that systems of records on individuals operated on their behalf under contracts be operated in conformance with the Act may be civilly liable to individuals injured as a consequence of any subsequent failure to maintain records in conformance with the Act."). Allowing 50 states to pile on and impose liability on contractors, with the financial consequences falling back on federal agencies in contract negotiations as the *Boyle* Court foresaw, might be found to upset the balance intended by Congress.

KeyPoint, however, has not argued for preemption—only for sovereign immunity. So, while it may press these arguments at future stages of litigation, we need not resolve the issue now.

* * *

This brings me to a final issue—the propriety of five plaintiffs proceeding under pseudonyms. Although some of our sister circuits take the view that a court of appeals has no jurisdiction over plaintiffs who "fail[] to request permission from the district court before proceeding anonymously," *W.N.J. v. Yocom*, 257 F.3d 1171, 1172 (10th Cir. 2001); accord, e.g., *United States ex rel. Little v. Triumph Gear Systems, Inc.*, 870 F.3d 1242, 1249–50 (10th Cir. 2017); *Citizens for a Strong Ohio v. Marsh*, 123 F. App'x 630, 636–37 (6th Cir. 2005); *Nat'l Commodity & Barter Ass'n v. Gibbs*, 886 F.2d 1240, 1245 (10th Cir. 1989) (per curiam), that doctrine, if adopted by us (which it has not been), would not change our handling of this appeal's merits—given the presence of other, non-pseudonymous plaintiffs. Moreover, the five anonymous plaintiffs in this case, see Arnold Plaintiffs' Compl. ¶¶ 22–26, J.A. 44–48, offer reasons that seem highly likely to prove worthy of district court permission—once they request it. But because pseudonymous filing impinges on values key to fair adjudication and a free society, it is hard to see how the district court on remand can avoid the issue once it has been noticed.

Although pseudonymous plaintiffs were once a rarity, there appears now to be a trend permitting adult plaintiffs to litigate incognito, with little more than pro-forma gatekeeping, if any, by the district courts—even though the practice is aberrant from the perspective of core constitutional and rule of law norms, not to mention the federal rules of procedure.

Under the "customary and constitutionally-embedded presumption of openness" that inheres in the nature of an Anglo-American trial, those who invoke the state's coercive apparatus must do so openly, i.e., under "their real names." *United States v. Microsoft Corp.*, 56 F.3d 1448, 1464 (D.C. Cir. 1995) (citations omitted); accord, e.g., *Doe v. Blue Cross & Blue Shield United*, 112 F.3d 869, 872 (7th Cir. 1997) (Posner,

J.) ("The people have a right to know who is using their courts."). For good reason. Public openness may "cause all trial participants to perform their duties more conscientiously," "induce unknown witnesses to come forward with relevant testimony," *Gannett Co. v. DePasquale*, 443 U.S. 368, 383 (1979), and generally foster "an appearance of fairness, thereby heightening respect for the judicial process," *Globe Newspaper Co. v. Superior Court for Norfolk Cnty.*, 457 U.S. 596, 606 (1982), cf. *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 569–73 (1980) (explaining importance of openness in criminal trial context). Of course, it's less important that respect for the judicial process be "heighten[ed]" than that it be *deserved*, which is less likely if plaintiffs can routinely act anonymously. In short, public scrutiny is essential to "the integrity of judicial proceedings." *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 665 (D.C. Cir. 2017) (quoting *United States v. Hubbard*, 650 F.2d 293, 315 (D.C. Cir. 1980)).

Indeed, it is a matter of "[b]asic fairness." *Microsoft*, 56 F.3d at 1463 (quoting *Southern Methodist Univ. Ass'n of Women Law Students v. Wynne & Jaffe*, 599 F.2d 707, 713 (5th Cir. 1979)). A case brought anonymously can let a winning plaintiff inflict "disgrace" on a defendant and can let a losing plaintiff launch defamatory charges "without shame or liability," *Doe v. Smith*, 429 F.3d 706, 710 (7th Cir. 2005); see also *Wynne*, 599 F.2d at 713; even in situations less drastic than *Doe v. Smith*, allowance of anonymity creates a structural asymmetry that can tilt the scales unfairly. If defendants get named, plaintiffs should too.

The principle of openness is far from an "arcane relic of ancient English law." *Hubbard*, 650 F.2d at 315 n.79 (citation omitted). Rule 10(a) of the civil rules says straightforwardly that the "title of [a] complaint *must* name *all* the parties." Fed.

R. Civ. P. 10(a) (emphases added). Perhaps "name" might be taken to mean something like "real or fictitious name." Cf. Carol M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, 57 U. Pitt. L. Rev. 883, 914–15 (1996) (denying that Rule 10(a) bars anonymous filings). This reading is questionable, not least because it appears to prove too much—it would mean that plaintiffs may proceed anonymously *as of right*, obviating a need for judicial approval or balancing, as discussed below. And Rule 10(a) contains no exception "for good cause," which features in many other contexts. See, e.g., Fed. R. Civ. P. 5(d)(3)(A), 6(c)(1)(C), 16(b)(4), 31(a)(5), 43(a); see also *Triumph Gear*, 870 F.3d at 1249 (stating that the federal rules "make no provision for suits by persons using fictitious names or for anonymous plaintiffs" (quoting *Commodity & Barter Ass'n*, 886 F.2d at 1245)); cf. *McKeever v. Barr*, 920 F.3d 842, 845 (D.C. Cir. 2019) (holding that when a rule of criminal procedure says "must," and provides no "residual exception," as the rules do elsewhere, the district court has no inherent power to create its own "exceptions").

Following our sister circuits, we've said in dictum that—even though anonymous filing is "an extraordinary break with precedent," *Microsoft*, 56 F.3d at 1464—a district court has discretion to "grant the 'rare dispensation' of anonymity against the world," *id*. (quoting *James v. Jacobson*, 6 F.3d 233, 238 (4th Cir. 1993)); cf. *Doe v. Frank*, 951 F.2d 320, 323 (11th Cir. 1992) ("It is the exceptional case in which a plaintiff may proceed under a fictitious name."). But, we explained, this "rare dispensation" can be granted only after the district court has conducted an inquiry into whether the circumstances justify an "extraordinary break" with the normal method of proceeding—openly—in federal court. *Microsoft*, 56 F.3d at 1464.

Anonymity for "rare" or "extraordinary" cases doesn't appear to be an apt description of current practice. Cf., e.g., *Coe v. Cnty. of Cook*, 162 F.3d 491, 498 (7th Cir. 1998) (Posner, J.) (criticizing the "overuse of pseudonyms in federal litigation"). Consider that in the twenty-five-year period between 1945 and 1969, only a single district court decision—anywhere in the country—featured a "John Doe"-like plaintiff as the lead or sole plaintiff (along with a single Supreme Court case reviewing a state court decision and three appellate rulings in administrative appeals). Adam A. Milani, *Doe v. Roe: An Argument for Defendant Anonymity When a Pseudonymous Plaintiffs Alleges a Stigmatizing Intentional Tort*, 41 Wayne L. Rev. 1659, 1660 (1995); see also Joan Steinman, *Public Trial, Pseudonymous Parties*, 37 Hastings L.J. 1, 1 n.2 (1985). And in the fifty years since that time, we have never "expressly condoned [the] practice." *Qualls v. Rumsfeld*, 228 F.R.D. 8, 9 (D.D.C. 2005). Yet there are now "two different but analogous tests . . . applied in this circuit" to rule on anonymity requests, *John Doe Co. v. Consumer Fin. Prot. Bureau*, 321 F.R.D. 31, 33 (D.D.C. 2017)—a six-factor test drawn from *United States v. Hubbard*, 650 F.2d 293, 317–21 (D.C. Cir. 1980), and a five-factor test elaborated in *National Association of Waterfront Employers v. Chao*, 587 F. Supp. 2d 90, 99 (D.D.C. 2008). Just last year, in this district alone, at least six published district court decisions featured "John Doe" as the lead or sole plaintiff.[1] That is to say nothing of the twenty or so other orders that permitted Doe and the like to (anonymously) level

[1] See *Doe 2 v. Trump*, 315 F. Supp. 3d 474 (D.D.C. 2018), *rev'd on other grounds sub nom. Doe 2 v. Shanahan*, 755 F. App'x 19 (D.C. Cir. 2019); *Doe 1 v. Buratai*, 318 F. Supp. 3d 218 (D.D.C. 2018); *Doe v. George Washington Univ.*, 305 F. Supp. 3d 126 (D.D.C. 2018); *Doe 1 v. FCC*, 302 F. Supp. 3d 160 (D.D.C. 2018); *Doe v. Mattis*, 288 F. Supp. 3d 195 (D.D.C. 2018); *Does 1–144 v. Chiquita Brands Int'l, Inc.*, 285 F. Supp. 3d 228 (D.D.C. 2018).

accusations against others; many of those orders were sealed[2] or lacked any reasoning at all (thereby omitting the "inquiry" required by *Microsoft*).[3] But cf., e.g., *EEOC v. Nat'l Children's Center, Inc.*, 98 F.3d 1406, 1410 (D.C. Cir. 1996) ("[I]t is imperative that a district court articulate its reasons for electing to seal or not to seal a record.").

Proceedings in this case appear to have gone yet further down the slope of anonymity. Here, five "Does" not only filed anonymously; they evidently never even bothered to *ask* the district court for permission to do so. The "docket sheet does not reflect any motion or proceeding dealing with whether" John Does I–III or Jane Does I–II "could proceed under pseudonyms." *Marsh*, 123 F. App'x at 636–37. In their amended Complaint the anonymous plaintiffs simply *announce*, in present participle form, that (for example) John Doe II "is using" a pseudonym "because of his personal safety concerns," as if such a cursory and conclusory statement suffices as belated justification in lieu of a court's permission. Arnold Plaintiffs' Compl. ¶ 25, J.A. 46. That simply cannot

---

[2] See *Zelda v. Sessions*, No. 1:18-cv-1966 (D.D.C. Aug. 22, 2018), ECF No. 2; *Voe v. Mattis*, No. 1:18-cv-1251 (D.D.C. June 6, 2018), ECF Nos. 8–9; *Kurd v. Repub. of Turkey*, No. 1:18-cv-1117 (D.D.C. May 11, 2018), ECF No. 4; *Doe A-1 v. Democratic People's Repub. of Korea*, No. 1:18-cv252 (D.D.C. Feb. 1, 2018), ECF No. 3.

[3] See *Garcia Ramirez v. ICE*, No. 1:18-cv-508 (D.D.C. Aug, 30, 2018) (minute order); *Dora v. Sessions*, No. 1:18-cv-1938 (D.D.C. Aug. 17, 2018), ECF No. 2; *Usoyan v. Repub. of Turkey*, No. 1:18-cv-1141 (D.D.C. May 15, 2018), ECF No. 5; *Damus v. Nielsen*, No. 1:18-cv-578 (D.D.C. Mar. 15, 2018), ECF No. 2; *Doe v. Kettler Mgmt., Inc.*, No. 1:18-cv-585 (D.D.C. Mar. 15, 2018), ECF No. 3; *Doe v. George Washington Univ.*, No. 1:18-cv-553 (D.D.C. Mar. 8, 2018), ECF No. 2; *Doe v. Kipp DC Supporting Corp.*, No. 1:18-cv-260 (D.D.C. Feb. 2, 2018), ECF No. 2; *Doe v. Syrian Arab Repub.*, No. 1:18-cv-66 (D.D.C. Jan. 11, 2018), ECF No. 2.

square with the federal rules or our longstanding commitment to openness, much less the rule referred to earlier of treating failure to *request* permission as fatal to jurisdiction over such parties.

On remand, then, the district court should consider the substantive and procedural questions relating to the Does' status in the lawsuit.

RULE 32 CERTIFICATION

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

The brief contains 11,858 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

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.

This the 24th day of June, 2019.

/s/ *Christopher T. Nace*
Christopher T. Nace, Esq.
Counsel for Appellants

United States Court of Appeals
for the District of Columbia Circuit

Chantal Attias, et al v. CareFirst, Inc., et al., No. 19-7020

CERTIFICATE OF SERVICE

I, Robyn Cocho, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

Counsel Press was retained by THE GIATRAS LAW FIRM, PLLC, Attorneys for Appellants to print this document. I am an employee of Counsel Press.

On **June 24, 2019,** counsel has authorized me to electronically file the foregoing **Brief of Appellants** with the Clerk of Court using the CM/ECF System, which will serve, via e-mail notice of such filing, to any of the following counsel registered as CM/ECF users:

MATTHEW GATEWOOD
EVERSHEDS SUTHERLAND (US) LLP
700 6th Street, NW, Suite 700
Washington, DC 20001-3980
(202) 383-0100
mattgatewood@eversheds-sutherland.com

ROBERT D. OWEN
EVERSHEDS SUTHERLAND (US) LLP
1114 Avenue of the Americas
Grace Building, 40th Floor
New York, NY 10036
(212) 389-5000
robertowen@eversheds-sutherland.com

A courtesy copy has also been mailed to the above listed counsel.

Unless otherwise noted, 8 paper copies have been filed with the Court on the same date via Express Mail.

June 24, 2019

/s/ Robyn Cocho
Robyn Cocho
Counsel Press