No. _____

In the Supreme Court of the United States

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., *et al.*,
Petitioners,

v.

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

On Petition for a Writ of Certiorari to the United States Court of Appeals for District of Columbia Circuit

PETITION FOR A WRIT OF CERTIORARI

Robert D. Owen
Francis X. Nolan, IV
EVERSHEDS SUTHERLAND (US) LLP
1114 Avenue of the Americas
The Grace Building
40th Floor
New York, NY 10036
T. 212.389.5000
F. 212.389.5099

Matthew O. Gatewood
Counsel of Record
EVERSHEDS SUTHERLAND (US) LLP
700 Sixth St., NW, Suite 700
Washington, D.C. 20001
T. 202.383.0122
F. 202.637.3593
MatthewGatewood@eversheds-sutherland.com

Counsel for Petitioners

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

QUESTION PRESENTED

Whether a plaintiff has Article III standing based on a substantial risk of harm that is not imminent and where the alleged future harm requires speculation about the choices of third-party actors not before the court.

PARTIES TO THE PROCEEDINGS AND RULE 29.6 STATEMENT

Petitioners, who were Defendants - Appellees below, are: 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.; 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.

Respondents, who were Plaintiffs - Appellants below, are: 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; Connie Tringler, Individually and on behalf of all others similarly situated.

Petitioner CareFirst, Inc., has no parent company. No publicly held company owns 10% or more of CareFirst, Inc. Petitioner CareFirst of Maryland, Inc., is a wholly owned subsidiary of CareFirst, Inc. Petitioner Group Hospitalization and Medical Services, Inc., is a wholly owned subsidiary of CareFirst, Inc. Petitioner CareFirst BlueChoice, Inc., is a wholly owned subsidiary of CareFirst, Inc.

TABLE OF CONTENTS

QUESTION PRESENTED i

PARTIES TO THE PROCEEDINGS AND RULE 29.6 STATEMENT ii

TABLE OF AUTHORITIES vi

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 1

STATEMENT OF JURISDICTION 1

CONSTITUTIONAL PROVISION INVOLVED . . . 1

STATEMENT OF THE CASE 2

a. Factual Background and District Court Proceedings. 3

b. The D.C. Circuit's Opinion. 5

REASONS FOR GRANTING THE PETITION 7

a. The Court of Appeals Erroneously Based Article III Standing on Asserted Injuries That Are Conjectural and Not Imminent. . . . 8

b. The D.C. Circuit's Holding Creates a Circuit Conflict on an Important Issue of Article III Standing. 10

c. The Question Presented Is Important, Frequently Recurring, and Cleanly Presented. 15

CONCLUSION 17

APPENDIX

Appendix A Opinion and Judgment in the United States Court of Appeals for the District of Columbia Circuit (August 1, 2017) . . . . . App. 1

Appendix B Memorandum Opinion and Order in the United States District Court for the District of Columbia (August 10, 2016) . . . . . App. 21

TABLE OF AUTHORITIES

CASES

In re Adobe Sys., Inc. Privacy Litig.,
66 F. Supp. 3d (N.D. Cal. 2014) 12

Ariz. Christian Sch. Tuition Org. v. Winn,
563 U.S. 125 (2011) 16

AT&T Mobility LLC v. Concepcion,
563 U.S. 333 (2011) 16

Beck v. McDonald,
848 F.3d 262 (4th Cir. 2017) 10, 11

Chambliss v. CareFirst, Inc.,
189 F. Supp. 3d (D. Md. 2016) 11, 13

Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013) . . . . . *passim*

Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.,
528 U.S. 167 (2000) 7

Galaria v. Nationwide Ins. Co.,
663 Fed. App'x 384 (6th Cir. 2016) 14

In re Idaho Conservation League,
811 F.3d 502 (D.C. Cir. 2016) 9

Katz v. Pershing, LLC,
672 F.3d 64 (1st Cir. 2012) 10

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 14

Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016) 14

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 2, 7

Monsanto Co. v. Geertson Seed Farms,
561 U.S. 139 (2010) 2

Nat'l Ass'n of Broadcasters v. FCC,
789 F.3d 165 (D.C. Cir. 2015) 9

Remijas v. Neiman Marcus,
794 F.3d 688 (7th Cir. 2015) 12, 13

Reilly v. Ceridian Corp.,
664 F.3d 38 (3d Cir. 2011), *cert. denied*,
132 S. Ct. 2395 (2012) 11

Sierra Club v. Jewell,
764 F.3d 1 (D.C. Cir. 2014) 9

In re SuperValu, Inc.,
870 F.3d 763 (2017) 10, 11, 12

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014) 8, 9

Unchageri v. CareFirst of Maryland, Inc.,
No. 1:16-cv-1068-MMM-JEH, 2016 WL 8255012
(C.D. Ill. Aug. 23, 2016) 13, 14

U.S. v. Jones,
565 U.S. 400 (2012) 15

Whalen v. Michaels Stores, Inc.,
689 Fed. Appx. 89 (2d Cir. 2017) 14

Whitmore v. Arkansas,
495 U.S. 149 (1990) 2

CONSTITUTION AND STATUTES

U.S. Const. art. III . . . . . *passim*

28 U.S.C. § 1254(1) 1

OTHER AUTHORITIES

Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 Gonz. L. Rev. 59 (2017) 15

Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. Cal. L. Rev. 683 (2017) 15

Michael Riley & Jordan Robertson, Bloomberg, *Chinese State-Sponsored Hackers Suspected in Anthem Attack* (Feb. 5, 2015), https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack 10

Eric C. Surette, *Liability of Businesses to Governments and Consumers for Breach of Data Security for Consumers' Information*, 1 A.L.R.7th Art. 2 (2015) 15

PETITION FOR A WRIT OF CERTIORARI

Petitioners CareFirst, Inc., Group Hospitalization and Medical Services, Inc., CareFirst of Maryland, Inc., Carefirst BlueCross BlueShield, CareFirst BlueChoice, Inc. (collectively "CareFirst"), respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the District of Columbia Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra* 1-20) is reported at 865 F.3d 620. The order of the district court (App., *infra* 21-36) granting defendants' motion to dismiss plaintiffs' second amended complaint is reported at 199 F. Supp. 3d 193.

STATEMENT OF JURISDICTION

The judgment of the court of appeals was entered on August 1, 2017. The Court's jurisdiction rests on 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

Article III, Section 2 of the U.S. Constitution provides that "[t]he judicial Power shall extend to all Cases, in Law and Equity, arising under * * * the Laws of the United States * * *."

STATEMENT OF THE CASE

The requirement that an alleged injury be actual or imminent is a bedrock principle of Article III standing necessary to invoke federal court jurisdiction. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013) (citing *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). For alleged future injuries, the Court restated in *Clapper* that "imminence" is satisfied when the threatened injury is "certainly impending." 568 U.S. 398, 402 (2013) (citing *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The Court acknowledged that a plaintiff can have standing when there is a "substantial risk" that a future injury will occur, but the Court did not hold that the substantial risk standard obviates the requirement that the alleged injury be imminent. *Id.* at 414 n.5. Regardless of the standard's name, federal courts are bound by the principle that Article III standing does not exist for an injury that requires an "attenuated chain of inferences necessary to find harm" or "speculation about 'the unfettered choices of independent actors not before the court.'" *Ibid.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 562 (1992)). Such "'allegations of *possible* future injury' are not sufficient." *Id.* at 409 (quoting *Whitmore*, 495 U.S. 158 (emphasis in *Clapper*)).

In this case, the D.C. Circuit's interpretation of the Court's "substantial risk" test does not meet the Article III requirement that an injury must be actual or imminent. *See id*. at 414 n.5 (quoting *Monsanto*, 561 U.S. at 153). The court of appeals concluded that in the context of alleged injuries arising from a data theft, "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." App. 16 (emphasis added). The D.C. Circuit's approach reduces the substantial risk standard to one of plausibility, a far less stringent test than even the objectively reasonable likelihood standard that the Court found inadequate in *Clapper*. 568 U.S. at 410. The D.C. Circuit's understanding of Article III standing for threatened injury is irreconcilable with the Court's jurisprudence and the decisions of numerous lower courts, including opinions from the Third, Fourth, and Eighth Circuits that involved allegations of future harm arising from data thefts.

The rising tide of data hacks and the class action lawsuits they inevitably spur increasingly test the boundaries of federal court jurisdiction. But lower courts have struggled to consistently apply Article III standing principles to future injuries allegedly caused by data theft, including the increased risk of future identity theft. Without guidance, courts, litigants, cybersecurity insurers, and corporate America will remain uncertain as to when a federal court can hear such claims.

This case presents an ideal vehicle for the Court to clarify that to satisfy the substantial risk standard, an alleged future injury must be imminent.

a. Factual Background and District Court Proceedings.

CareFirst is a national health insurance company, and it insures respondents. In June 2014, an unknown thief or thieves hacked CareFirst's electronic servers and accessed certain data. The hackers potentially accessed respondents' names, birth dates, email

addresses, and subscriber identification numbers. CareFirst promptly notified its policyholders when it discovered the breach in May 2015.

Respondents instituted a putative class action against CareFirst shortly thereafter, alleging that CareFirst failed to protect their information, thus exposing them to possible future identity theft. App. 3. The complaint alleges that CareFirst maintained Social Security numbers and other Personally Identifiable Information ("PII"), *ibid.*, but it does not allege that the thieves accessed Social Security numbers or such other PII. *Id.* at 22 n.1. CareFirst submitted an affidavit in support of its motion to dismiss confirming that the breached databases did not contain respondents' Social Security numbers or credit card numbers. *Id.* at 22.

The district court held that "[a]bsent facts demonstrating a substantial risk that stolen data has been or will be used in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from which the information was stolen." App. 23. The district court found that respondents' "theory of injury is * * * too speculative to satisfy *Clapper*," *id.* at 29, including because the complaint does not allege how the data thieves could commit identity theft based

on the information they accessed.[1] *Ibid.* The district court concluded it lacked subject matter jurisdiction because respondents did not have Article III standing.

b. The D.C. Circuit's Opinion.

The court of appeals reversed the district court, finding that respondents faced a "substantial risk of future injury," App. 11, fairly traceable to CareFirst's alleged failure to properly secure the accessed data.[2] *Id.* at 16.

To reach this holding, the court of appeals concluded that the district court erred in finding that the complaint did not allege the theft of Social Security numbers or credit card numbers. *Id.* at 13-14. The court of appeals found that the complaint alleged that: (1) CareFirst collects that information, *id.* at 13; (2) "PII/PHI/Sensitive Information," as defined by the respondents, includes that information, *ibid.*; (3) the data theft "allowed access to PII, PHI, ePHI, and other personal and sensitive information," *ibid.*; and (4) the

---

[1] The district court also assumed that two respondents (the Tringlers) pled an injury-in-fact by alleging tax-refund fraud, but held they could not fairly trace their injury to the CareFirst breach based on the data they alleged was stolen. *Id.* at 31. The Tringlers' specific claims of injury were not germane to the D.C. Circuit's analysis. App. 10 n.2 ("Because we conclude that all plaintiffs, including the Tringlers, have standing to sue CareFirst based on their heightened risk of future identity theft, we need not address the Tringlers' separate argument as to *past* identity theft.") (emphasis in original).

[2] The court of appeals first held that the district court's order, although not explicitly with prejudice, was final and appealable. App. 8.

information "including that accessed on Defendants' servers" can be used by thieves to "commit various * * * financial misdeeds." *Ibid*. Taking these allegations together, "the complaint thus *plausibly* alleges that the CareFirst data breach exposed customers' social security and credit card numbers." *Id.* at 14 (emphasis added).

The court of appeals did not consider that respondents have not suffered any identity theft or other harm in more than three years since the breach. Separately, the court of appeals found that, even if Social Security numbers and credit card numbers had not been accessed, the complaint's allegation that "a combination of members' names, birth dates, email addresses and subscriber identification numbers alone qualifies as personal information, and the unauthorized access to said combination of information creates a material risk of identity theft" was enough to confer Article III standing. *Ibid.* The court of appeals reasoned that a thief could use this information to "impersonate" one of the CareFirst policyholders in order to "obtain[] medical services in her name." *Ibid.* Respondents' complaint does not allege this theory, which they raised for the first time on appeal.

This petition followed.

REASONS FOR GRANTING THE PETITION

To establish standing (and thus federal jurisdiction) under Article III, a plaintiff bears the burden of showing that he or she "(1) * * * has suffered an 'injury in fact' that is (a) concrete and particularized and (b) *actual or imminent*, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 180–81 (2000) (emphasis added). The injury-in-fact requirement is an "irreducible constitutional minimum" for standing. *Defenders of Wildlife*, 504 U.S. at 560–61 (1992). "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes." *Id.* at 564–65 n.2. The Court has set forth standards for evaluating the imminence requirement, including the certainly impending and substantial risk tests. *Clapper*, 568 U.S. at 414 n.5. The Court has not held that these tests differ in any material respect.

The court of appeals, however, explicitly differentiated between the "substantial risk" and "certainly impending" standards when analyzing allegations of future injury. App. 11 ("*either* the 'certainly impending' test *or* the 'substantial risk' test") (emphasis in original). Further, unlike other courts that have applied the substantial risk standard, the court of appeals did not consider whether the alleged future threat was imminent, or whether respondents had spent money on mitigation damages. The D.C.

Circuit's interpretation of the substantial risk standard eviscerates the fundamental requirement that an injury be imminent for Article III standing to exist. The court's holding cannot be reconciled with this Court's Article III standing jurisprudence and is in conflict with other courts of appeals.

a. The Court of Appeals Erroneously Based Article III Standing on Asserted Injuries That Are Conjectural and Not Imminent.

The court of appeals did not analyze whether respondents' alleged future injuries were "certainly impending," as the Court did in *Clapper*. 568 U.S. at 402. Instead, citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (2014), the court of appeals applied the "substantial risk" standard. App. 12. The substantial risk test, however, is no less demanding than the certainly impending test. Furthermore, the risk of future identity theft is not the type of substantial risk previously contemplated by the Court. *S.B.A. List* and its progeny primarily involved allegations of risks of extreme injury or impending government actions that

would result from acts of the plaintiffs themselves.[3] Those risks were not dependent on the acts of unknown third parties, as is the case here.

Even the court of appeals noted that any threat to respondents is based entirely on future possible acts of unknown third parties. App. 14 (finding that there is a "substantial risk of identity theft if [respondents'] social security and credit card numbers were accessed by a network intruder" by virtue of the nature of the data); *ibid.* (finding it "*plausible*" that thieves could use a "combination of members' names, birth dates, email addresses and subscriber identification number[s]" to "impersonate[] [respondents] and obtain[] medical services in [their] name[s]") (emphasis added). The court of appeals did not require these future potential injuries to be "imminent," and noted only that "it is much less speculative—at the very least, it is *plausible*—to infer that [the thief] has both the intent and the ability to use that data for ill." *Id.* at 15 (emphasis added); *see also ibid.* (finding that there is "a *plausible* allegation that plaintiffs face a substantial risk of identity fraud, even if their social security

---

[3] *See* App. 12 (citing *In re Idaho Conservation League*, 811 F.3d 502, 509 (D.C. Cir. 2016) (finding that one of the plaintiffs alleged an injury-in-fact based on present harm arising from arsenic mine waste, and substantial risk of similar future harm if a not-yet-constructed mine was completed as planned); *Nat'l Ass'n of Broadcasters v. FCC*, 789 F.3d 165, 181 (D.C. Cir. 2015) (finding that the plaintiff had alleged substantial risk of future injury to challenge the timing of the FCC's implementation of a framework that would necessarily impact the plaintiff's television stations); *Sierra Club v. Jewell*, 764 F.3d 1, 7 (D.C. Cir. 2014) (finding that individuals who would not be able to view a historic battlefield if coal mining proceeded on the land as planned)).

numbers were never exposed to the data thief") (emphasis added).

By holding the respondents to a plausibility standard and a "light burden of proof * * * at the pleading stage," *id.* at 12, the court of appeals failed to heed the Court's warning that standing does not exist where a future injury relies entirely on a "highly attenuated chain of possibilities." *Clapper*, 568 U.S. at 410. The D.C. Circuit's lower Article III threshold for threatened injury is irreconcilable with the Court's precedent, particularly given the amount of time that has passed since the 2014 breach, and other possible motivations of the unknown thieves that the court of appeals failed to consider. *See, e.g.*, Michael Riley & Jordan Robertson, Bloomberg, *Chinese State-Sponsored Hackers Suspected in Anthem Attack* (Feb. 5, 2015), https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack.

b. The D.C. Circuit's Holding Creates a Circuit Conflict on an Important Issue of Article III Standing.

The courts of appeals are "divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft." *Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017); *see also Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) ("The courts of appeals have evidenced some disarray about the applicability of this sort of 'increased risk' theory [of injury] in data privacy cases."); *In re SuperValu, Inc.*, 870 F.3d 763, 769 (2017) ("These cases came to differing conclusions on the question of standing.").

Even in light of the circuit split, the D.C. Circuit entered uncharted territory by finding that "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." App. 16. That holding is plainly at odds with at least the Third, Fourth, and Eighth Circuits, which have held that a plaintiff does not have standing based on an increased risk of identity theft absent an allegation of actual harm. Any of those courts would have upheld the district court's dismissal given the absence of an imminent injury.

The Third Circuit has held that allegations of future injury are too remote, and not sufficiently "imminent," when "dependent on entirely speculative, future actions of an unknown third party." *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012); *id.* at 43 ("we cannot describe how [plaintiffs] will be injured in this case without beginning our explanation with the word 'if'"). The Fourth Circuit interpreted *Clapper* to stand for the "common-sense notion that a threatened event can be 'reasonably likely' to occur but still be insufficiently 'imminent' to constitute an injury-in-fact." *Beck*, 848 F.3d at 276. The *Beck* court found that the allegations of impending future harm were undermined by the fact that the plaintiffs had not suffered identity theft in the three-to-four years following the two subject breaches. *Id.* at 274–75 (citing *Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016)).

In *In re Supervalu, Inc.*, the Eighth Circuit dismissed the plaintiffs' claims that arose from allegations of future injury that were not combined with allegations of actual, present injury. 870 F.3d at

770. The plaintiffs in *Supervalu* submitted a Government Accounting Office ("GAO") report in support of their contention that "data breaches facilitate identity theft," *id.* at 767, 770, but the GAO report concluded that "most breaches have not resulted in detected incidents of identity theft." *Id.* at 771.

Decisions from other circuit courts, although reconcilable with the district court's dismissal in this case, reflect a growing uncertainty as to what is required to plead a future injury-in-fact. For example, in *Remijas v. Neiman Marcus*, where the plaintiff alleged that credit card numbers were stolen from the defendant department store's database, resulting in fraudulent charges to the accounts of at least 9,200 putative class members, the Seventh Circuit did not need to speculate as to the data thieves' future intentions. 794 F.3d 688, 689–90 (7th Cir. 2015). The *Remijas* court distinguished between *Clapper*'s "certainly impending" and "substantial risk" standards, relying on the Court's statement that the latter standard is implicated where a party "reasonably incur[s] costs to mitigate or avoid that [future] harm." *Id.* at 693 (quoting *Clapper*, 568 U.S. at 414 n.5). Unlike the D.C. Circuit, however, the Seventh Circuit did not remove the imminence requirement from the substantial risk analysis. In fact, the Seventh Circuit specifically focused on whether the alleged future injuries were "immediate and very real," including by analyzing the data that was stolen and how it had been used since the theft. *Ibid.* (quoting *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)). The Seventh Circuit posed a rhetorical question, quoted by the court of appeals here: "Why else would hackers break into a store's database and

steal consumers' private information?" *Ibid.* In the context of stolen credit card numbers and the ensuing fraudulent charges to nearly 10,000 consumers, the logic of that question rang true in *Remijas*. In this case, however, it does not.

The existing circuit court split is highlighted by conflicting results in nearly identical cases brought against CareFirst in different jurisdictions but arising from the same data theft that gave rise to this claim. In *Chambliss v. CareFirst, Inc.*, the District of Maryland noted that the CareFirst breach "compromised only Plaintiffs' names, birthdates, email addresses, and subscriber identification numbers, and not their social security numbers, credit card information, or any other similarly sensitive data that could heighten the risk of harm." 189 F. Supp. 3d at 570. Unlike the court of appeals here, the *Chambliss* court also understood that the "certainly impending" and "substantial risk" standards both require that the alleged future injury be imminent. *Id.* at 569. Where the future injury is dependent "on the actions of an unknown independent party it creates a theory of injury that only amounts to an 'objectively reasonable likelihood'" of future harm, a standard that the Court in *Clapper* rejected. *Ibid.* The *Chambliss* court also pointed out that the further in the past the CareFirst breach faded, the "imminence of the asserted harm * * * becomes ever less likely." *Id.* at 570 (citations omitted).

Three months later, in *Unchageri v. CareFirst of Maryland, Inc.*, the Central District of Illinois, following the Seventh Circuit's guidance from *Remijas* and *Lewert*, found no standing because the plaintiffs

did not allege "any *present* injuries to show that the risk of future harm is certainly impending." No. 1:16-cv-1068-MMM-JEH, 2016 WL 8255012, at * 6 (C.D. Ill. Aug. 23, 2016) (emphasis in original). There was no misuse of data at the time of the filing of the complaint, so the future injury could not have been "certainly impending." *Ibid.* (based on data allegedly stolen in the CareFirst data theft, "allegations of *possible* future injury are not sufficient" for standing) (quoting *Clapper*, 568 U.S. at 410).

The discord among lower courts over what constitutes an imminent future injury-in-fact for Article III standing will continue to grow without guidance from the Court. *See Galaria v. Nationwide Ins. Co.*, 663 Fed. App'x 384, 386 (6th Cir. 2016) (finding substantial risk of future injury where Social Security numbers were stolen and plaintiffs incurred mitigation costs in the form of credit protection services); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (in pre-*Clapper* decision, holding that a "credible threat" of future identity theft was enough, even where plaintiffs did not allege why a laptop containing their PII was stolen, the identity of the thief, or whether the thief knew that the laptop contained PII); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) (finding standing where third party data thieves stole plaintiffs' credit and debit card data from defendant, and plaintiffs incurred charges to mitigate damages from potential future identity theft); *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89, 90 (2d Cir. 2017) (finding that plaintiff "does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other

personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen").

c. The Question Presented Is Important, Frequently Recurring, and Cleanly Presented.

It is well-chronicled that "[c]yberattacks that cause widespread data breaches are more prevalent now than ever before." Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 Gonz. L. Rev. 59, 60 (2017); *see also* Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. Cal. L. Rev. 683, 685 (2017) ("In 2016, there were 1,093 data breaches, up from 780 in 2015. 75.6% of companies suffered at least one successful attack.") (citations omitted). Unsurprisingly, lawsuits are often filed by consumers after a breach becomes public, "and especially class action lawsuits." Eric C. Surette, *Liability of Businesses to Governments and Consumers for Breach of Data Security for Consumers' Information*, 1 A.L.R.7th Art. 2 (2015).

Given the number and scope of cyberattacks, there is potential for enormous liability despite the fact that many resulting lawsuits do not arise from actual, concrete harm to the plaintiffs who file them. Standing is especially critical to consistently apply given the constant redefinition of concepts such as privacy and security in the digital age, where private information exists in multiple forms, is under constant assault, and 100% security is impossible. *See, e.g.*, *U.S. v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (noting that we live "in the digital age, in which people

reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

If a putative class action survives just long enough for a class to be certified, liability and actual damages often become largely irrelevant in determining settlement value. "When damages allegedly owed to tens of thousands of potential claimants are aggregated and decided at once, the risk of an error will often become unacceptable. Faced with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011).

With these ramifications in mind, the Court should provide guidance to the lower courts on the boundaries of federal court jurisdiction to hear these claims. As the Court has noted, we live in an "era of frequent litigation [and] class actions [so] courts must be more careful to insist on the formal rules of standing, not less so." *Ariz. Christian Sch. Tuition Org. v. Winn*, 563 U.S. 125, 146 (2011). The D.C. Circuit's holding that the respondents' "cleared the *low bar to establish their standing*," App. 2 (emphasis added), directly threatens to erode the fundamental requirement that a federal court can hear only claims alleging harms that are actual or imminent.

The decision of the court of appeals is incorrect, has exacerbated a circuit split, and cleanly presents significant and purely legal questions for the Court's review. The allegations here provide an ideal opportunity to clarify that the substantial risk standard requires a threatened injury to be imminent,

just as the Court has clarified when determining whether threatened injury is certainly impending.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Robert D. Owen
Francis X. Nolan, IV
EVERSHEDS SUTHERLAND (US) LLP
1114 Avenue of the Americas
The Grace Building
40th Floor
New York, NY 10036
T. 212.389.5000
F. 212.389.5099

Matthew O. Gatewood
Counsel of Record
EVERSHEDS SUTHERLAND (US) LLP
700 Sixth St., NW
Suite 700
Washington, D.C. 20001
T. 202.383.0122
F. 202.637.3593
MatthewGatewood@eversheds-sutherland.com

Counsel for Petitioners

APPENDIX

APPENDIX

TABLE OF CONTENTS

Appendix A Opinion and Judgment in the United States Court of Appeals for the District of Columbia Circuit (August 1, 2017) . . . . . App. 1

Appendix B Memorandum Opinion and Order in the United States District Court for the District of Columbia (August 10, 2016) . . . . . App. 21

APPENDIX A

UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 16-7108

[Filed August 1, 2017]

CHANTAL ATTIAS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL., 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., ET AL., APPELLEES	)

Argued March 31, 2017 Decided August 1, 2017

Appeal from the United States District Court
for the District of Columbia
(No. 1:15-cv-00882)

Jonathan B. Nace argued the cause for appellants. With him on the briefs was *Christopher T. Nace.*

Marc Rotenberg and *Alan Butler* were on the brief for *amicus curiae* Electronic Privacy Information Center (EPIC) in support of appellants.

Tracy D. Rezvani was on the brief for *amicus curiae* National Consumers League in support of appellants.

Matthew O. Gatewood argued the cause for appellees. With him on the briefs was *Robert D. Owen*.

Andrew J. Pincus, *Stephen C.N. Lilley*, *Kathryn Comerford Todd*, *Steven P. Lehotsky*, and *Warren Postman* were on the brief for *amicus curiae* The Chamber of Commerce of the United States of America in support of appellees.

Before: TATEL, GRIFFITH, and MILLETT, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* GRIFFITH.

GRIFFITH, *Circuit Judge*: In 2014, health insurer CareFirst suffered a cyberattack in which its customers' personal information was allegedly stolen. A group of CareFirst customers attributed the breach to the company's carelessness and brought a putative class action. The district court dismissed for lack of standing, finding the risk of future injury to the plaintiffs too speculative to establish injury in fact. We conclude that the district court gave the complaint an unduly narrow reading. Plaintiffs have cleared the low bar to establish their standing at the pleading stage. We accordingly reverse.

I

CareFirst and its subsidiaries are a group of health insurance companies serving approximately one million customers in the District of Columbia, Maryland, and Virginia.[1] When customers purchased CareFirst's insurance policies, they provided personal information to the company, including their names, birthdates, email addresses, social security numbers, and credit card information. CareFirst then assigned each customer a subscriber identification number. The companies stored this information on their servers. Allegedly, though, CareFirst failed to properly encrypt some of the data entrusted to its care.

In June 2014, an unknown intruder breached twenty-two CareFirst computers and reached a database containing its customers' personal information. CareFirst did not discover the breach until April 2015 and only notified its customers in May 2015. Shortly after the announcement, seven CareFirst customers brought a class action against CareFirst and its subsidiaries in our district court. Their complaint invoked diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), and raised eleven different state-law causes of action, including breach of contract, negligence, and violation of various state consumer-protection statutes.

The parties disagree over what the complaint alleged. According to CareFirst, the complaint alleged only the exposure of limited identifying data, such as

---

[1] The facts in this section are primarily taken from the plaintiffs' second amended complaint.

customer names, addresses, and subscriber ID numbers. According to plaintiffs, the complaint also alleged the theft of customers' social security numbers. The plaintiffs sought to certify a class consisting of all CareFirst customers residing in the District of Columbia, Maryland, and Virginia whose personal information had been hacked. CareFirst moved to dismiss for lack of Article III standing and, in the alternative, for failure to state a claim.

The district court agreed that the plaintiffs lacked standing, holding that they had alleged neither a present injury nor a high enough likelihood of future injury. The plaintiffs had argued that they suffered an increased risk of identity theft as a result of the data breach, but the district court found this theory of injury to be too speculative. The district court did not read the complaint to allege the theft of social security numbers or credit card numbers, and concluded that "[p]laintiffs have not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers." *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 201 (D.D.C. 2016).

Based on its determination that the plaintiffs had failed to allege an injury in fact, the district court ordered that their "[c]omplaint be dismissed without prejudice." J.A. 350 (emphasis omitted). The court did not decide whether diversity jurisdiction was proper, or whether the plaintiffs had stated a claim for which relief could be granted. Plaintiffs timely appealed.

II

Although the parties agree that we have jurisdiction to hear this appeal, we have an independent duty to ensure that we are acting within the limits of our authority. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 93-94 (1998). Our jurisdiction embraces "appeals from all *final* decisions of the district courts of the United States." 28 U.S.C. § 1291 (emphasis added). In evaluating the finality of district court rulings on motions to dismiss, we have distinguished between orders dismissing the *action*, which are final, *see Ciralsky v. CIA*, 355 F.3d 661, 666 (D.C. Cir. 2004), and orders dismissing the *complaint*, which, if rendered "without prejudice," are "typically" not final, *Murray v. Gilmore*, 406 F.3d 708, 712 (D.C. Cir. 2005). But here, even though the district court ordered that the plaintiffs' "[c]omplaint be dismissed without prejudice," J.A. 350 (emphasis omitted), we are convinced that its order was final, and that we have jurisdiction over this appeal.

Key to that conclusion are the district court's grounds for dismissal. The court below concluded that it lacked subject-matter jurisdiction because the plaintiffs lacked Article III standing. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (identifying the plaintiff's Article III standing as an element of federal courts' jurisdiction). When a court lacks subject-matter jurisdiction, it has no authority to address the dispute presented. "Jurisdiction is the power to declare the law, and when it ceases to exist, the only function remaining to the court is that of announcing the fact and dismissing the cause." *Steel Co.*, 523 U.S. at 94 (quoting *Ex parte McCardle*, 74 U.S.

(7 Wall.) 506, 514 (1868)). Thus, in the ordinary case, a dismissal for lack of subject-matter jurisdiction ends the litigation and leaves nothing more for the court to do. That is the definition of a final, appealable order. *See Riley v. Kennedy*, 553 U.S. 406, 419 (2008). This principle fits neatly into the *Ciralsky-Murray* framework: a dismissal for lack of subject-matter jurisdiction is, in effect, a dismissal of the *action*, and therefore final, even if, as here, it is styled as a dismissal of the complaint. *See Tootle v. Sec'y of Navy*, 446 F.3d 167, 172 (D.C. Cir. 2006) ("A district court must dismiss an action where . . . it concludes that it lacks subject matter jurisdiction.").

But that rule is flexible, and we recognize, as did the *Ciralsky* court, that the district court's intent is a significant factor in the analysis. *See* 355 F.3d at 667-68. Thus, if the district court intended for the action to continue via amendment of the complaint to allege facts supporting jurisdiction, its dismissal order is not final. *See Murray*, 406 F.3d at 712-13.

To accommodate both the rule that a dismissal for lack of subject-matter jurisdiction ordinarily ends the action and the need to respect the intentions of the district court that entered the order, we will presume, absent a clear indication to the contrary, that a dismissal for lack of subject-matter jurisdiction under Rule 12(b)(1) is a final, appealable order. Other circuits have similarly concluded that a district court's dismissal for lack of subject-matter jurisdiction is generally final and appealable. *See, e.g.*, *Radha Geismann, M.D., P.C. v. ZocDoc, Inc.*, 850 F.3d 507, 509 n.3 (2d Cir. 2017); *City of Yorkville ex rel. Aurora Blacktop Inc. v. Am. S. Ins. Co.*, 654 F.3d 713, 715-16

(7th Cir. 2011); *Whisnant v. United States*, 400 F.3d 1177, 1180 (9th Cir. 2005).

Where subject-matter jurisdiction depends on the factual allegations in the complaint, as it does here, the district court can signal that a dismissal under Rule 12(b)(1) is not final if it expressly gives the plaintiff leave to amend the complaint. *See* FED. R. CIV. P. 15(a)(2). A court that has extended such an invitation to amend clearly contemplates that there is still some work for the court to do before the litigation is over. *See Riley*, 553 U.S. at 419; *see also Mohawk Indus., Inc. v. Carpenter*, 558 U.S. 100, 106 (2009) (describing a final decision as one "by which a district court disassociates itself from a case" (quoting *Swint v. Chambers Cty. Comm'n*, 514 U.S. 35, 42 (1995))).

On the other hand, a court's statement that its jurisdictional dismissal is "without prejudice" will not, by itself, overcome the presumption that such dismissals terminate the *action*, not just the complaint. By dismissing without prejudice, a district court leaves the plaintiff free to return later to the same court with the same underlying claim. *See Semtek Int'l Inc. v. Lockheed Martin Corp.*, 531 U.S. 497, 505 (2001). But as *Ciralsky* explained, either a complaint or an action can be dismissed "without prejudice." *See* 355 F.3d at 666-67. Thus, an order of dismissal "without prejudice" tells us nothing about whether the district court intended to dismiss the *action*, which would be a final order, or the *complaint*, which would not. By contrast, an express invitation to amend is a much clearer signal that the district court is rejecting only the *complaint* presented, and that it intends the action to continue.

Though it may be possible in some cases to discern an invitation to amend the complaint from clues in the district court's opinion, we think that anything less than an *express* invitation is not a clear enough signal to overcome the presumption of finality. This approach balances the district court's position as master of its docket, *see Dietz v. Bouldin*, 136 S. Ct. 1885, 1892 (2016); *Cunningham v. Hamilton Cty.*, 527 U.S. 198, 203 (1999), our supervisory authority, *see Ciralsky*, 355 F.3d at 667 (noting that we are not bound to accept a district court's determination that its order *is* final), and the need for clarity in assessing the finality of an order, *cf. id.* ("[I]t is not always clear whether a district court intended its order to dismiss the action or merely the complaint.").

Because the district court in this case dismissed for lack of subject-matter jurisdiction without expressly inviting the plaintiffs to amend their complaint or giving some other equally clear signal that it intended the action to continue, the order under review ended the district court action, and was thus final and appealable. We have appellate jurisdiction under 28 U.S.C. § 1291.

III

We now turn to the question the district court decided and which we review de novo: whether the plaintiffs have standing to bring their action against CareFirst. *See Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 913 (D.C. Cir. 2015). Standing is a prerequisite to the existence of a "Case[]" or "Controvers[y]," which is itself a precondition to the exercise of federal judicial power. U.S. CONST. art. III, §§ 1-2; *Lujan*, 504 U.S. at 560. To demonstrate

standing, a plaintiff must show that she has suffered an "injury in fact" that is "fairly traceable" to the defendant's actions and that is "likely to be redressed" by the relief she seeks. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (quoting *Lujan*, 504 U.S. at 560).

The burden to make all of these showings always remains with the plaintiff, but the burden grows as the litigation progresses. *Lujan*, 504 U.S. at 561. The district court dismissed this action at the pleading stage, where plaintiffs are required only to "state a *plausible* claim" that each of the standing elements is present. *See Food & Water Watch*, 808 F.3d at 913 (emphasis added) (quoting *Humane Soc'y of the U.S. v. Vilsack*, 797 F.3d 4, 8 (D.C. Cir. 2015)); *see also Lujan*, 504 U.S. at 561 ("[E]ach element [of standing] must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation. At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice . . . ." (citations omitted)).

This case primarily concerns the injury-in-fact requirement, which serves to ensure that the plaintiff has a personal stake in the litigation. *See Susan B. Anthony List v. Driehaus* (*SBA List*), 134 S. Ct. 2334, 2341 (2014). An injury in fact must be concrete, particularized, and, most importantly for our purposes, "actual or imminent" rather than speculative. *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560).

The district court found missing the requirement that the plaintiffs' injury be "actual or imminent." *Id.* The plaintiffs here alleged that the data breach at CareFirst exposed them to a heightened risk of identity theft. The principal question, then, is whether the

plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.[2]

As the district court recognized, the leading case on claims of standing based on risk of future injury is *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). In *Clapper*, plaintiffs challenged a provision of the Foreign Intelligence Surveillance Act that allowed surveillance of foreign nationals outside the United States. *Id.* at 404-05 (citing 50 U.S.C. § 1881a). Though the plaintiffs were not foreign nationals, they alleged an "objectively reasonable likelihood" that their communications with overseas contacts would be intercepted. *Id.* at 410. The Court responded that "threatened injury must be certainly impending to constitute injury in fact." *Id.* (quoting *Whitmore v.*

---

[2] Two of the plaintiffs, Curt and Connie Tringler, alleged that they had already suffered identity theft as a result of the breach. Specifically, they claimed that their anticipated tax refund had gone missing. The district court acknowledged that the Tringlers had alleged an injury in fact but held that the Tringlers nevertheless lacked standing because their injury was not fairly traceable to the data breach. On the district court's reading, the complaint did not allege theft of social security numbers, and the Tringlers had not explained how thieves could divert a tax refund without access to the taxpayers' social security numbers.

Because we conclude that all plaintiffs, including the Tringlers, have standing to sue CareFirst based on their heightened risk of future identity theft, we need not address the Tringlers' separate argument as to *past* identity theft. For the same reason, we will not address the other theories of standing advanced by plaintiffs or their *amici*, including the theory that CareFirst's alleged violation of state consumer protection statutes was a distinct injury in fact.

Arkansas, 495 U.S. 149, 158 (1990)). But the Court also noted that in some cases it has "found standing based on a 'substantial risk' that the harm will occur." *Id.* at 414 n.5.

The plaintiffs' theory of standing in *Clapper*, however, failed under either formulation. *Id.* at 410, 414 n.5. The major flaw in their argument was that it rested on "a highly attenuated chain of possibilities." *Id.* at 410. Several links in this chain would have required the assumption that independent decisionmakers charged with policy discretion (*i.e.*, executive-branch intelligence officials) and with resolving complex legal and factual questions (*i.e.*, the Article III judges of the Foreign Intelligence Surveillance Court) would exercise their discretion in a specific way. *See id.* at 410-14. With so many links in the causal chain, the injury the plaintiffs feared was too speculative to qualify as "injury in fact."

In *Susan B. Anthony List v. Driehaus*, the Court clarified that a plaintiff can establish standing by satisfying *either* the "certainly impending" test *or* the "substantial risk" test. *See* 134 S. Ct. at 2341. The Court held that an advocacy group had standing to bring a pre-enforcement challenge to an Ohio statute prohibiting false statements during election campaigns. *See id.* at 2347. The holding rested in part on the fact that the group could conceivably face criminal prosecution under the statute, *id.* at 2346, but the Court also described the risk of administrative enforcement, standing alone, as "substantial," *id.* This was so even though any future enforcement proceedings would be based on a complaint not yet made regarding a statement the group had not yet

uttered against a candidate not yet identified. *See id.* at 2343-45.

Since *SBA List*, we have frequently upheld claims of standing based on allegations of a "substantial risk" of future injury. *See, e.g.*, *In re Idaho Conservation League*, 811 F.3d 502, 509 (D.C. Cir. 2016) (using "significant risk" and "reasonabl[e] fears" as the standard); *Nat'l Ass'n of Broadcasters v. FCC*, 789 F.3d 165, 181 (D.C. Cir. 2015) (using "substantial risk"); *Sierra Club v. Jewell*, 764 F.3d 1, 7 (D.C. Cir. 2014) (using "substantial probability of injury"). Under our precedent, "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case would be identity theft, "as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes." *Food & Water Watch*, 808 F.3d at 915 (quoting *Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1298 (D.C. Cir. 2007)).

Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury. The remaining question, then, keeping in mind the light burden of proof the plaintiffs bear at the pleading stage, is whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach. *See id.*

We start with the familiar principle that the factual allegations in the complaint are assumed to be true at the motion-to-dismiss stage. *See, e.g.*, *Jerome Stevens*

Pharms., Inc. v. FDA, 402 F.3d 1249, 1253-54 (D.C. Cir. 2005); *see also Food & Water Watch*, 808 F.3d at 913 (noting that we need not "assume the truth of legal conclusions[or] accept inferences that are unsupported by the facts set out in the complaint" (quoting *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015))). The district court concluded that the plaintiffs had "not demonstrated a sufficiently substantial risk of future harm stemming from the breach to establish standing," *Attias*, 199 F. Supp. 3d at 201, in part because they had "not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers," *id.* But that conclusion rested on an incorrect premise: that the complaint did not allege the theft of social security or credit card numbers in the data breach. In fact, the complaint did.

The complaint alleged that CareFirst, as part of its business, collects and stores its customers' personal identification information, personal health information, and other sensitive information, all of which the plaintiffs refer to collectively as "PII/PHI/Sensitive Information." J.A. 7. This category of "PII/PHI/ Sensitive Information," as plaintiffs define it, includes "patient credit card . . . and social security numbers." J.A. 7. Next, the complaint asserted that "the cyberattack [on CareFirst] allowed access to PII, PHI, ePHI, and other personal and sensitive information of Plaintiffs." J.A. 8. And, according to the plaintiffs, "[i]dentity thieves can use identifying data—*including that accessed on Defendants' servers*—to open new financial accounts[,] incur charges in another person's name," and commit various other financial misdeeds; the CareFirst breach exposed "all of the information

wrongdoers need" for appropriation of a victim's identity. *See* J.A. 5, 11 (emphasis added).

So we have specific allegations in the complaint that CareFirst collected and stored "PII/PHI/Sensitive Information," a category of information that includes credit card and social security numbers; that PII, PHI, and sensitive information were stolen in the breach; and that the data "accessed on Defendants' servers" place plaintiffs at a high risk of financial fraud. The complaint thus plausibly alleges that the CareFirst data breach exposed customers' social security and credit card numbers. CareFirst does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their social security and credit card numbers were accessed by a network intruder, and, drawing on "experience and common sense," we agree. *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

The complaint separately alleges that the "combination of members' names, birth dates, email addresses and subscriber identification number[s] *alone* qualifies as personal information, and the unauthorized access to said combination of information creates a material risk of identity theft." J.A. 8 (emphasis added). This allegation of risk based solely on theft of health insurance subscriber ID numbers is plausible when taken in conjunction with the complaint's description of a form of "medical identity theft" in which a fraudster impersonates the victim and obtains medical services in her name. *See* J.A. 12. That sort of fraud leads to "inaccurate entries in [victims'] medical records" and "can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance,

or become disqualified from some jobs." J.A. 12. These portions of the complaint would make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identity fraud, even if their social security numbers were never exposed to the data thief.

Our conclusion that the alleged risk here is "substantial" is bolstered by a comparison between this case and the circumstances in *Clapper*. In *Clapper*, the plaintiffs feared the interception of their overseas communications by the government, but that harm could only occur through the happening of a series of contingent events, none of which was alleged to have occurred by the time of the lawsuit. *See* 568 U.S. at 410-14. The harm also would not have arisen unless a series of independent actors, including intelligence officials and Article III judges, exercised their independent judgment in a specific way. Even then, the intelligence officials would need to have actually captured the plaintiffs' conversations in the process of targeting those plaintiffs' foreign contacts. *See id.*

Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill. As the Seventh Circuit asked, in another data breach case where the court found standing, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015). No long sequence of

uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken. That risk is much more substantial than the risk presented to the *Clapper* Court, and satisfies the requirement of an injury in fact.

Of course, plaintiffs cannot establish standing merely by alleging that they have been injured. An alleged injury in fact must also be "fairly traceable to the challenged conduct of the defendant." *Spokeo*, 136 S. Ct. at 1547. Though CareFirst devotes only limited space in its brief to this point, the company argues that the plaintiffs "do not allege that the thief is or was in any way affiliated with CareFirst." Appellees' Br. 7. The company thus seems to contend that the plaintiffs' injury is "fairly traceable" only to the data thief. It is of course true that the thief would be the most immediate cause of plaintiffs' injuries, should they occur, and that CareFirst's failure to secure its customers' data would be one step removed in the causal chain. But Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be "fairly traceable" to the defendant. *See Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1391 n.6 (2014); *Orangeburg v. FERC*, No. 15-1274, 2017 WL 2989486, at *6 (D.C. Cir. July 14, 2017). 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, *see, e.g.*, *Public*

Citizen, 489 F.3d at 1289, we have little difficulty concluding that their injury in fact is fairly traceable to CareFirst.

Finally, the plaintiffs' injury must be "likely to be redressed by a favorable judicial decision." *Spokeo*, 136 S. Ct. at 1547. *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.

IV

CareFirst urges us, in the alternative, to hold that the plaintiffs' complaint fails to state a claim for which relief can be granted. *See* FED. R. CIV. P. 12(b)(6). However, an antecedent question remains: whether the plaintiffs properly invoked the district court's diversity jurisdiction under 28 U.S.C. § 1332. The district court expressly reserved judgment on that issue, and on the

record before us, we cannot answer it ourselves. It would thus be inappropriate for us to reach beyond the standing question.

Accordingly, the district court's order dismissing this action for lack of standing is reversed, and the case is remanded for further proceedings consistent with this opinion.

So ordered.

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 16-7108

[Filed August 1, 2017]

CHANTAL ATTIAS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL., 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., ET AL., APPELLEES	)

September Term, 2016
FILED ON: August 1, 2017

Appeal from the United States District Court
for the District of Columbia
(No. 1:15-cv-00882)

Before: TATEL, GRIFFITH, and MILLETT, *Circuit Judges*.

J U D G M E N T

This cause came on to be heard on the record on appeal from the United States District Court for the District of Columbia and was argued by counsel. On consideration thereof, it is

ORDERED and **ADJUDGED** that the District Court's order dismissing this action for lack of standing be reversed and the case be remanded for further proceedings, in accordance with the opinion of the court filed herein this date.

Per Curiam

FOR THE COURT:
Mark J. Langer, Clerk

BY: /s/
Ken Meadows
Deputy Clerk

Date: August 1, 2017

Opinion for the court filed by Circuit Judge Griffith.

APPENDIX B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Case No. 15-cv-00882 (CRC)

[Filed August 10, 2016]

CHANTAL ATTIAS, et al.,)
Plaintiffs,)
)
v.)
)
CAREFIRST, INC., et al.,)
Defendants.)

MEMORANDUM OPINION

Theft of electronic data has become commonplace in our digital economy, victimizing millions of Americans each year. But while the resulting harm to consumers can be catastrophic, not all data breaches result in legally actionable injuries. As a result, when consumers whose data has been compromised seek redress in the courts, it must be determined whether their alleged injuries are sufficiently specific and concrete to give them standing to sue. That is the task presently before the Court in this case.

In June 2014, the health insurer CareFirst suffered a data breach that compromised the personal information of some 1.1 million policyholders, including the seven named Plaintiffs here. The purloined

information included the policyholders' names, birth dates, email addresses, and subscriber identification numbers. Compl. ¶ 32; see also Defs.' Reply Ex. 1 (Decl. Clayton Moore House) ¶ 10. According to CareFirst, more-sensitive data, such as social security and credit card numbers, was not stolen.[1] After CareFirst publicly acknowledged the breach in May 2015, Plaintiffs sued the company and various of its affiliates on behalf of themselves and other policyholders, alleging that CareFirst violated a host of state laws and legal duties by failing to safeguard their personal information.[2] Another set of plaintiffs filed a similar federal class action in Maryland.

CareFirst has moved to dismiss Plaintiffs' complaint. It argues that because Plaintiffs have not alleged that their personal information has actually been misused, or explained how the stolen information could readily be used to assume their identities, they lack standing to sue in federal court. Plaintiffs mainly respond that the increased likelihood of identity theft that resulted from the breach, and the costs they have

---

[1] Although Plaintiffs assert in their opposition to the motion to dismiss that their social security numbers were stolen in the data breach, the Complaint neither makes that allegation explicitly nor contains any factual contentions that would support that conclusion. See Pls.' Opp'n 17 (citing Compl. ¶ 57).

[2] Plaintiffs allege that the Court has jurisdiction over the case pursuant to 28 U.S.C. § 1332(d)(2) because the class's aggregate claims exceed $5,000,000 and "there are numerous class members who are citizens of states other than the Defendants." Compl. ¶ 10. The Court will not assess this assertion because, as discussed below, it will dismiss the case for lack of subject matter jurisdiction on standing grounds.

incurred to mitigate it, are sufficient injuries to establish standing. In resolving this dispute, the Court will follow the standard set by the majority of courts that have confronted similar cases, including the related Maryland class action: Absent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from whom the information was taken. Because Plaintiffs have not made the required showing, the Court lacks subject matter jurisdiction over the case and will grant CareFirst's motion to dismiss.

I. Legal Standard

Defendants move to dismiss the Complaint for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) and for failure to state a claim upon which relief can be granted pursuant to Rule 12(b)(6). "The distinctions between 12(b)(1) and 12(b)(6) are important and well understood. Rule 12(b)(1) presents a threshold challenge to the court's jurisdiction, whereas 12(b)(6) presents a ruling on the merits with res judicata effect." Al-Owhali v. Ashcroft, 279 F. Supp. 2d 13, 20 (D.D.C. 2003) (quoting Haase v. Sessions, 835 F.2d 902, 906 (D.C.Cir.1987)) (internal quotation marks omitted). Because "a court must begin with questions of jurisdiction" "[b]efore examining the merits of any claim," In re Sci. Applications Int'l Corp. ("SAIC"), 45 F. Supp. 3d 14, 23 (D.D.C. 2014), and because the Court will conclude that it lacks subject matter jurisdiction, this Opinion will address only Defendants' jurisdictional arguments. Thus, "Federal Rule of Civil Procedure 12(b)(1) provides the relevant

legal standard." Id. at 22. Under this standard, the Court must "treat the [C]omplaint's factual allegations as true . . . and must grant [Plaintiffs] the benefit of all inferences that can be derived from the facts alleged." Id. (omission in original) (quoting Sparrow v. United Air Lines, Inc., 216 F.3d 1111, 1113 (D.C. Cir. 2000)) (internal quotation marks omitted).

At the same time, because a "court has an 'affirmative obligation to ensure that it is acting within the scope of its jurisdictional authority,'" id. at 23 (quoting Grand Lodge of Fraternal Order of Police v. Ashcroft, 185 F. Supp. 2d 9, 13 (D.D.C. 2001)), a plaintiff's factual allegations in the complaint "will bear closer scrutiny in resolving a 12(b)(1) motion than in resolving a 12(b)(6) motion for failure to state a claim," id. (quoting Grand Lodge, 185 F. Supp. 2d at 13–14) (internal quotation mark omitted). "Additionally, unlike with a motion to dismiss under Rule 12(b)(6), the Court 'may consider materials outside the pleadings in deciding whether to grant a motion to dismiss for lack of jurisdiction.'"[3] Id. (quoting Jerome Stevens Pharm. v. FDA, 402 F.3d 1249, 1253 (D.C. Cir. 2005)).

II. Analysis

Article III of the U.S. Constitution limits the reach of federal jurisdiction to the resolution of cases and controversies. See U.S. Const. art. III, § 2. "Because 'standing is an essential and unchanging part of the

[3] For this reason, the Court will consider, and deny, Plaintiffs' motion to strike the affidavit of CareFirst IT security official Clayton Moore House, which details the parameters of the data breach.

case-or-controversy requirement of Article III,'" SAIC, 45 F. Supp. 3d at 23 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)), "standing is a necessary 'predicate to any exercise of [the Court's] jurisdiction,'" id. (alteration in original) (quoting Fla. Audubon Soc'y v. Bentsen, 94 F.3d 658, 663 (D.C. Cir. 1996)). Consequently, every federal court plaintiff "bears the burden of establishing the three elements that make up the irreducible constitutional minimum of Article III standing: injury-in-fact, causation, and redressability." Id. (quoting Dominguez v. UAL Corp., 666 F.3d 1359, 1362 (D.C. Cir. 2012)) (internal quotation marks omitted). "Even in the class-action context, all named Plaintiffs must allege and show that they personally have been injured." Id. (quoting Warth v. Seldin, 422 U.S. 490, 502 (1975)) (internal quotation mark omitted). And plaintiffs must plead or prove, "with the requisite 'degree of evidence required at the successive stages of the litigation,'" each element of standing. Id. (quoting Lujan, 504 U.S. at 561). Thus, "at the motion-to-dismiss stage, Plaintiffs must plead facts that, taken as true, make the existence of standing plausible." Id.

The question at issue here is whether the named Plaintiffs have demonstrated an "injury in fact" that is concrete, particularized, and actual or imminent, Lujan, 504 U.S. at 560 (quoting Allen v. Wright, 468 U.S. 737, 756 (1984)) (internal quotation marks omitted), and, if so, whether that injury is "fairly traceable" to the CareFirst data breach, id. at 590 (alteration omitted) (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41 (1976)) (internal quotation mark omitted). With the exception of two of the Plaintiffs—Kirk and Connie Tringler, who will be

discussed below—none allege that they have suffered actual identity theft.[4] They contend instead that they have been harmed because the data breach has increased the likelihood that they will be the victims of identity theft in the future. In assessing such prospective harms, the Supreme Court held in Clapper v. Amnesty International USA that "[a]llegations of *possible* future injury" do not satisfy constitutional standing requirements. 133 S. Ct. 1138, 1147 (2013) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158

---

[4] Although the Plaintiffs' opposition to the Defendants' motion to dismiss asserts that "*many* Plaintiffs have already suffered identity theft, credit card fraud, and had their tax returns stolen," Pls.' Opp'n 5 (emphasis added) (citing Compl. ¶¶ 47–57), and that victims of the data breach other than the Tringlers have suffered "actual identity theft and fraud," id. at 3 (citing Compl. ¶ 57), the Complaint contains no factual allegations to support those assertions. The paragraphs of the Complaint Plaintiffs cite contain only conjecture regarding Plaintiffs other than the Tringlers. See Compl. ¶ 49 ("Identity thieves *can* use identifying data . . . to open new financial accounts and incur charges in another person's name . . . ." (emphasis added)); id. ¶ 50 ("Identity thieves *can* use personal information . . . to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, ..." (emphasis added)); id. ¶ 51 ("[I]dentity thieves *may* get medical services using the Plaintiff's PII [Personally Identifiable Information] and PHI [Personal Health Information] or commit any number of other frauds . . . ." (emphasis added)); id. ¶ 55 ("Identity thieves *can* use [stolen] information" to enroll unwilling beneficiaries into certain health plans. (emphasis added)). Because a "complaint may not be amended by the briefs in opposition to a motion to dismiss," BEG Invs., LLC v. Alberti, 85 F. Supp. 3d 13, 26 (D.D.C. 2015) (quoting Coleman v. Pension Benefit Guar. Corp., 94 F. Supp. 2d 18, 24 n.8 (D.D.C. 2000)) (internal quotation marks omitted), Plaintiffs' assertion of harm in their opposition does not constitute an allegation mounted in the Complaint.

(1990)) (internal quotation marks omitted). Rather, the "threatened injury must be *certainly impending* to constitute injury in fact." Id. (quoting Whitmore, 495 U.S. at 158) (internal quotation marks omitted). That does not mean that Plaintiffs are required to show that it is "literally certain that the harms they identify will come about." Id. at 1150 n.5. But they must at least demonstrate a "'substantial risk' that the harm will occur." Id. (quoting Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2754–55 (2010)). Plaintiffs whose claim of injury depends on an "attenuated chain of inferences necessary to find harm" will "fall short" of the mark. Id. The Court turns to each of Plaintiffs' claimed injuries below.

A. Increased Risk of Identity Theft

Judge Boasberg of this Court recently applied Clapper's "certainly impending" standard to a claim of injury resulting from filched electronic data. SAIC, 45 F. Supp. 3d at 24. In that case, back-up tapes containing the personal information and medical records of military service members were among various items stolen from the car of an employee of the information technology company SAIC. See id. at 19–20. The data tapes originated with a federal agency that provides health insurance to military families, and SAIC was in possession of the tapes through an IT security contract with the agency. See id. Service members whose data was contained on the tapes sued, alleging in part that they had been harmed by the increased likelihood that they would suffer identity fraud as a result of the theft. See id.

The Court found the plaintiffs' claims of increased risk of identity theft to be insufficient to establish

injury in fact. Judge Boasberg reasoned that too many assumptions were required to find the alleged harm certainly impending. The thief would still need to "recognize the tapes for what they were"; "find a tape reader and attach it to her computer"; "acquire software to upload the data"; decipher any encrypted portions of the data; "acquire familiarity with the [health insurance company's] database format, which might require another round of special software"; and finally, "either misuse a particular Plaintiff's [information] or sell that Plaintiff's data to a willing buyer who would then abuse it." Id. at 25. Because the plaintiffs had not alleged that any of those things had occurred, and because those "events [were] entirely dependent on the actions of an unknown third party," they failed to demonstrate standing under Clapper. Id.

Plaintiffs attempt to distinguish SAIC by pointing out that, unlike the thieves there—who stole various physical objects from a car, some of which happened to contain data—those here breached CareFirst's server protections for the very purpose of accessing that data, thus demonstrating their intent to misuse it. See Pls.' Opp'n 10–11. Plaintiffs point to the Seventh Circuit's recent decision in Remijas v. Neiman Marcus Group, 794 F.3d 688 (7th Cir. 2015), as more-analogous precedent. Remijas involved a data breach of Neiman Marcus's computer systems, which compromised customers' credit card information, social security numbers, and birth dates. See id. at 690. Of the 350,000 credit cards whose information was potentially exposed, 9,200 "were known to have been used fraudulently." Id. In other words, the hackers had clearly demonstrated that they had the means and the will either to abuse the information they accessed or to

sell it to others who did so. Unlike in SAIC, where only two plaintiffs out of the 4.7 million service members whose information was stolen plausibly alleged an injury traceable to the theft, SAIC, 45 F. Supp. 3d at 31–33, in Remijas, even the plaintiffs who had not yet experienced fraud had demonstrated that they faced a "substantial risk" of fraud sufficient to confer standing because so many other plaintiffs had experienced cognizable harm traceable to the breach, Remijas, 794 F.3d at 693.

The Court views SAIC to be more similar to this case than Remijas and other data breach cases cited by Plaintiffs. See Pls.' Opp'n 6–10. While the series of assumptions required to find concrete harm to Plaintiffs may be somewhat shorter here than that in SAIC, their theory of injury is still too speculative to satisfy Clapper. The Court would have to assume, at a minimum, that the hackers have the ability to read and understand Plaintiffs' personal information, the intent to "commit future criminal acts by misusing the information," and the ability to "use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs'] names." Chambliss v. CareFirst, Inc., No. RDB-15-2288, 2016 WL 3055299, at *4 (D. Md. May 27, 2016) (alterations in original) (quoting In re SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016)) (internal quotation mark omitted). And, even more speculative than in SAIC—where social security numbers were among the stolen data—is the question whether the hackers here would be willing or able to use the existing data to acquire *additional* data. Plaintiffs have not suggested, let alone demonstrated, how the CareFirst hackers

could steal their identities without access to their social security or credit card numbers. See, e.g., Antman v. Uber Techs., Inc., No. 3:15-cv-01175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("[T]he court holds that Mr. Antman's allegations are not sufficient because his complaint alleges only the theft of names and driver's licenses. Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."). The absence of such a showing distinguishes this case from Remijas, where the demonstrated existence of thousands of unauthorized charges shortly following the data breach clearly established a connection between the breach and the thieves' ability and willingness to commit fraud.

The court in the related Maryland class action reached same conclusion, granting the defendants' motion to dismiss for lack of subject matter jurisdiction on standing grounds. It rejected the plaintiffs' argument that the breach increased their risk of future harm because "most courts to consider the issue 'have agreed that the mere loss of data—without any evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.'" Chambliss, 2016 WL 3055299, at *4 (quoting SAIC, 45 F. Supp. 3d at 19) (citing In re Zappos.com, Inc., 108 F.Supp.3d 949, 958–59 (D. Nev. 2015); Green v. eBay, Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015); In re Horizon Healthcare Servs., Inc. Data Breach Litig., No. 13-7418, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015); Key v. DSW, Inc., 454 F.Supp.2d 684, 689 (S.D. Ohio 2006)). The court added that "since Clapper[,] . . .

courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases." Id. (quoting SAIC, 45 F.Supp.3d at 28) (citing In re SuperValu, 2016 WL 81792, at *4); Strautins v. Trustwave Holdings, Inc., 27 F.Supp.3d 871, 876 (N.D. Ill. 2014)) (internal quotation marks omitted). This Court likewise concludes that Plaintiffs have not demonstrated a sufficiently substantial risk of future harm stemming from the breach to establish standing.

B. Actual Identity Theft

As noted above, two of the named Plaintiffs—Kirk and Connie Tringler—allege that they have already suffered an injury from the data breach. They claim that they have experienced tax-refund fraud in that they have still not received an expected tax refund. See Compl. ¶ 57. While suffering this type of fraud may constitute a concrete and particularized injury, in order to demonstrate standing, Plaintiffs must also plausibly assert that their alleged injury is "fairly traceable to the challenged action." Clapper, 133 S. Ct. at 1147. And again, while the Plaintiffs' opposition asserts that the stolen information included social security numbers, the Complaint does not support that allegation. See supra note 1; Pls.' Opp'n 17; Compl. ¶ 57. As Defendants point out, and Plaintiffs do not contest, "[i]t is not plausible that tax refund fraud could have been conducted without the Tringlers' Social Security Numbers." Defs. Reply 5; see also Furlow v. United States, 55 F. Supp. 2d 360, 362–63 (D. Md. 1999) ("[T]o receive an income tax exemption . . . , the taxpayer must include the social security number or taxpayer identification number of the claimed individual on his returns."). Therefore, the Tringlers have not plausibly

alleged that any tax-return fraud they have experienced is fairly traceable to the data breach.

C. Other Claimed Harms

In addition to arguing that the increased risk of future harm confers standing upon Plaintiffs other than the Tringlers and that the Tringlers have already experienced cognizable injury, all Plaintiffs contend that they have experienced four other types of harm: (1) economic harm through having to purchase credit-monitoring services to prevent identity theft and fraud; (2) economic harm through overpayment for their insurance coverage, the cost of which they maintain should have covered prophylactic measures against hacking; (3) loss of the intrinsic value of their personal information; and (4) violation of their statutory rights under consumer protection acts. None of the arguments in support of these contentions is availing.

First, because the increased risk of future identity theft or fraud is too speculative to confer standing, Plaintiffs cannot opt in to standing-conferring economic injury by purchasing protection from that future harm. Where "future harm . . . is not certainly impending," plaintiffs "cannot manufacture standing by choosing to make expenditures based on" that "hypothetical" harm. Clapper, 133 S. Ct. at 1143. In other words, Plaintiffs "cannot create standing by 'inflicting harm on themselves'" in the form of purchasing credit-monitoring services in order "to ward off an otherwise speculative injury." SAIC, 45 F. Supp. 3d at 26 (quoting Clapper, 133 S. Ct. at 1151).

Second, a claim that "some indeterminate part of their premiums went toward paying for security

measures . . . is too flimsy to support standing." Id. at 30. Like the plaintiffs in SAIC, Plaintiffs here "do not maintain that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime." Id. Nor have they "alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid." Id.

Third, also like the plaintiffs in SAIC, "Plaintiffs do not contend that *they* intended to sell [their personal] information on the cyber black market in the first place, so it is uncertain how they were injured" by the alleged loss of the intrinsic value of that information. Id. In addition, "it is unclear whether or how the data has been devalued by the breach." Id. Without factual allegations to support this contention, Plaintiffs do not plausibly assert harm from the loss of their personal information's intrinsic value.

Fourth, Plaintiffs contend that this Court must conclude that they have standing because the D.C. Court of Appeals, they assert, has held that a violation of the D.C. Consumer Protection Procedures Act can confer standing on its own. See Pls.' Opp'n 13 (citing Grayson v. AT&T Corp., 15 A.3d 219, 247 (D.C. 2011)). Setting aside the fact that only the Plaintiffs who are residents of the District of Columbia assert violations of this D.C. Act, statutory rights cannot confer Article III standing on a plaintiff who does not have it otherwise. See Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547–48 (2016) ("Injury in fact is a constitutional requirement, and '[i]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not

otherwise have standing.'" (alteration in original) (quoting Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997))). This is so because an injury in fact must be "both 'concrete *and* particularized.'" Id. at 1545 (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)). While violation of a plaintiff's statutory rights is not irrelevant to standing, it is also not sufficient because it "concern[s] particularization, not concreteness," id. at 1548: "Article III standing requires a concrete injury even in the context of a statutory violation," id. at 1549. And a "'concrete' injury must be '*de facto*'; that is, it must actually exist." Id. at 1548. Where a violation of a statute "may result in no harm," that mere violation is insufficient to confer standing. Id. at 1550. Even if Plaintiffs' rights under applicable consumer protection acts have been violated, because they do not plausibly allege concrete harm, they have not demonstrated that they have standing to press their claims.[5]

---

[5] Plaintiffs have filed a notice of supplemental authority flagging for the Court a recently decided D.C. Circuit case concerning an alleged violation of D.C. laws protecting consumers from the disclosure of contact information in the course of credit card transactions. See Hancock v. Urban Outfitters, Inc., No. 14-7047, 2016 WL 3996710 (D.C. Cir. July 26, 2016). The court held that the plaintiffs failed to establish standing because, although they alleged statutory violations, they did not allege any concrete injury in fact as a result of those violations. See id. at *6–7. In dicta, the court noted that "increased risk of fraud or identity theft . . . may satisfy Article III's requirement of concrete injury." Id. at *7. It is this statement that Plaintiffs emphasize in their notice. However, the D.C. Circuit's reasoning, and the principal that increased risk of harm *may* satisfy the constitutional requirement of concrete injury are entirely consistent with the Court's analysis here.

III. Conclusion

For the foregoing reasons, Defendants' motion to dismiss will be granted and the Second Amended Complaint dismissed without prejudice, and Plaintiffs' motion to strike will be denied. An order accompanies this memorandum opinion.

/s/ Christopher R. Cooper
CHRISTOPHER R. COOPER
United States District Judge

Date: August 10, 2016

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Case No. 15-cv-00882 (CRC)

[Filed August 10, 2016]

CHANTAL ATTIAS, et al.,	)
Plaintiffs,	)
	)
v.	)
	)
CAREFIRST, INC., et al.,	)
Defendants.	)
	)

ORDER

For the reasons stated in the accompanying Memorandum Opinion, it is hereby

ORDERED that [13] Defendants' Motion to Dismiss be **GRANTED**. It is further

ORDERED that [9] Plaintiffs' Second Amended Complaint be **DISMISSED WITHOUT PREJUDICE**. It is further

ORDERED that [17] Plaintiffs' Motion to Strike, or in the Alternative, Motion to Convert Motion to Dismiss to Motion for Summary Judgment be **DENIED**.

SO ORDERED.

/s/ Christopher R. Cooper
CHRISTOPHER R. COOPER
United States District Judge

Date: August 10, 2016