2017 WL 5041488 (U.S.) (Appellate Petition, Motion and Filing)
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.

No. 17-641.
October 30, 2017.

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, Eversheds Sutherland (US) LLP, 700 Sixth St., NW, Suite 700, Washington, D.C. 20001, T. 202.383.0122, F. 202.637.3593, Matthew Gatewood@eversheds-sutherland.com, for petitioners.

***i** 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.

***ii** 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.

***iii** 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.

*iv TABLE OF CONTENTS

*v APPENDIX

*vi TABLE OF AUTHORITIES

CASES

*vii

*viii CONSTITUTION AND STATUTES

OTHER AUTHORITIES

*1 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 ***."

*2 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 ***3** 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 ***4** 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 ***5** 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 ***6** 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.

***7 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. ***8** 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 ***9** 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 ***10** 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.").

***11** 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. ***12** 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 ***13** 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 ***14** 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 ***15** 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 ***16** 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, ***17** 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.

Footnotes

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.

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)).

End of Document