United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued March 31, 2017 Decided August 1, 2017

No. 16-7108

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

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,

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

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 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

[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.

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. 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.