EXHIBIT 1

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION,	No. 16-16860
	D.C. No. 3:12-cv-00325-RCJ-VPC
THERESA STEVENS; KRISTIN O'BRIEN; TERRI WADSWORTH; DAHLIA HABASHY; PATTI HASNER; SHARI SIMON; STEPHANIE PRIERA; KATHRYN VORHOFF; DENISE RELETHFORD; ROBERT REE, *Plaintiffs-Appellants*, v. ZAPPOS.COM., INC., *Defendant-Appellee.*	OPINION

Appeal from the United States District Court
for the District of Nevada
Robert Clive Jones, Senior District Judge, Presiding

Argued and Submitted December 5, 2017
San Francisco, California

Filed March 8, 2018

Before: John B. Owens and Michelle T. Friedland, Circuit Judges, and Elaine E. Bucklo,* District Judge.

Opinion by Judge Friedland

SUMMARY**

Article III Standing

The panel reversed the district court's dismissal, for lack of Article III standing, of plaintiffs' claims alleging that they were harmed by hacking of their accounts at the online retailer Zappos.com.

The panel held that under *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), plaintiffs sufficiently alleged standing based on the risk of identity theft. The panel rejected Zappos's argument that *Krottner* was no longer good law after *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). And the panel held that plaintiffs sufficiently alleged an injury in fact under *Krottner*, based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft. The panel assessed plaintiffs' standing as of the time the complaints were filed, not as of the present. The panel further held that plaintiffs sufficiently alleged that the risk of future harm they faced was "fairly traceable" to the conduct being challenged; and the risk from

* The Honorable Elaine E. Bucklo, United States District Judge for the Northern District of Illinois, sitting by designation.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

the injury of identity theft was also redressable by relief that could be obtained through this litigation.

The panel addressed an issue raised by sealed briefing in a concurrently filed memorandum disposition.

COUNSEL

Douglas Gregory Blankinship (argued), Finkelstein Blankinship Frei-Pearson and Garber LLP, White Plains, New York; David C. O'Mara, The O'Mara Law Firm P.C., Reno, Nevada; Ben Barnow, Barnow and Associates P.C., Chicago, Illinois; Richard L. Coffman, The Coffman Law Firm, Beaumont, Texas; Marc L. Godino, Glancy Binkow & Goldberg LLP, Los Angeles, California; for Plaintiffs-Appellants.

Stephen J. Newman (argued), David W. Moon, Brian C. Frontino, and Julia B. Strickland, Stroock & Stroock & Lavan LLP, Los Angeles, California; Robert McCoy, Kaempfer Crowell, Las Vegas, Nevada; for Defendant-Appellee.

OPINION

FRIEDLAND, Circuit Judge:

In January 2012, hackers breached the servers of online retailer Zappos.com, Inc. ("Zappos") and allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers. Several of those customers filed putative class actions in federal courts across the country, asserting that Zappos had not adequately protected their personal information. Their lawsuits were consolidated for pretrial proceedings.

Although some of the plaintiffs alleged that the hackers used stolen information about them to conduct subsequent financial transactions, the plaintiffs who are the focus of this appeal ("Plaintiffs") did not. This appeal concerns claims based on the hacking incident itself, not any subsequent illegal activity.

The district court dismissed Plaintiffs' claims for lack of Article III standing. In this appeal, Plaintiffs contend that the district court erred in doing so, and they press several potential bases for standing, including that the Zappos data breach put them at risk of identity theft.

We addressed standing in an analogous context in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). There, we held that employees of Starbucks had standing to sue the company based on the risk of identity theft they faced after a company laptop containing their personal information was stolen. *Id.* at 1140, 1143. We reject Zappos's argument that *Krottner* is no longer good law after *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), and hold that, under

Krottner, Plaintiffs have sufficiently alleged standing based on the risk of identity theft.[1]

I.

When they bought merchandise on Zappos's website, customers provided personal identifying information ("PII"), including their names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information. Sometime before January 16, 2012, hackers targeted Zappos's servers, stealing the PII of more than 24 million of its customers, including their full credit card numbers.[2] On January 16, Zappos sent an email to its customers, notifying them of the theft of their PII. The company recommended "that they reset their Zappos.com account passwords and change the passwords 'on any other web site where [they] use the same or a similar password.'" Some customers responded almost immediately by filing putative class actions in federal district courts across the country.

---

[1] We address an issue raised by sealed briefing in a concurrently filed memorandum disposition.

[2] Although Zappos asserts in its briefs that the hackers stole only the last four digits of customers' credit card numbers, it has presented its arguments as a facial, not a factual, attack on standing. *See Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004) (distinguishing facial from factual attacks on standing). Where, as here, "a defendant in its motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) asserts that the allegations in the complaint are insufficient to establish subject matter jurisdiction as a matter of law (to be distinguished from a claim that the allegations on which jurisdiction depends are not true as a matter of fact), we take the allegations in the plaintiff's complaint as true." *Whisnant v. United States*, 400 F.3d 1177, 1179 (9th Cir. 2005).

In these suits, Plaintiffs alleged an "imminent" risk of identity theft or fraud from the Zappos breach. Relying on definitions from the United States Government Accountability Office ("GAO"), they characterized "identity theft" and "identity fraud" as "encompassing various types of criminal activities, such as when PII is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud."[3]

The Judicial Panel on Multidistrict Litigation transferred several putative class action lawsuits alleging harms from the Zappos data breach to the District of Nevada for pretrial proceedings. After several years of pleadings-stage litigation, including a hiatus for mediation, the district court granted in part and denied in part Zappos's motion to dismiss the Third Amended Consolidated Complaint ("Complaint") and granted Zappos's motion to strike the Complaint's class allegations. The court distinguished between two groups of plaintiffs: (1) plaintiffs named only in the Third Amended Complaint who alleged that they had already suffered financial losses from identity theft caused by Zappos's breach, and (2) plaintiffs named in earlier complaints who did not allege having already suffered financial losses from identity theft.

[3] Plaintiffs did not provide a precise cite but appear to be referring to the description of identity theft in a report entitled *Personal Information*, which explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." U.S. Gov't Accountability Office, GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* 2 (2007).

The district court ruled that the first group of plaintiffs had Article III standing because they alleged "that actual fraud occurred as a direct result of the breach." But the court ruled that the second group of plaintiffs (again, here referred to as "Plaintiffs") lacked Article III standing and dismissed their claims without leave to amend because Plaintiffs had "failed to allege instances of actual identity theft or fraud." The parties then agreed to dismiss all remaining claims with prejudice, and Plaintiffs appealed.

II.

We review the district court's standing determination de novo. *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). To have Article III standing,

> a plaintiff must show (1) it 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. (TOC), Inc., 528 U.S. 167, 180–81 (2000); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). A plaintiff threatened with future injury has standing to sue "if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013)) (internal quotation marks omitted).

III.

We addressed the Article III standing of victims of data theft in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). In *Krottner*, a thief stole a laptop containing "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees." *Id.* at 1140. "Starbucks sent a letter to . . . affected employees alerting them to the theft and stating that Starbucks had no indication that the private information ha[d] been misused," but advising them to "monitor [their] financial accounts carefully for suspicious activity and take appropriate steps to protect [themselves] against potential identity theft." *Id.* at 1140–41 (internal quotation marks omitted). Some employees sued, and the only harm that most alleged was an "increased risk of future identity theft." *Id.* at 1142. We determined this was sufficient for Article III standing, holding that the plaintiffs had "alleged a credible threat of real and immediate harm" because the laptop with their PII had been stolen. *Id.* at 1143.

A.

Before analyzing whether *Krottner* controls this case, we must determine whether *Krottner* remains good law after the Supreme Court's more recent decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), which addressed a question of standing based on the risk of future harm.

As a three-judge panel, we are bound by opinions of our court on issues of federal law unless those opinions are "clearly irreconcilable" with a later decision by the Supreme Court. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). This is the first case to require us to consider

whether *Clapper* and *Krottner* are clearly irreconcilable, and we conclude that they are not.

The plaintiffs in *Clapper* challenged surveillance procedures authorized by the Foreign Intelligence Surveillance Act of 1978—specifically, in 50 U.S.C. § 1881a (2012) (amended 2018).[4] *Clapper*, 568 U.S. at 401. The plaintiffs, who were "attorneys and human rights, labor, legal, and media organizations whose work allegedly require[d] them to engage in sensitive and sometimes privileged telephone and e-mail communications with . . . individuals located abroad," sued for declaratory relief to invalidate § 1881a and an injunction against surveillance conducted pursuant to that section. *Id.* at 401, 406. The plaintiffs argued that they had Article III standing to challenge § 1881a "because there [was] an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future." *Id.* at 401. The Supreme Court rejected this basis for standing, explaining that "an objectively reasonable likelihood" of injury was insufficient, and that the alleged harm needed to "satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

[4] 50 U.S.C. § 1881a authorizes electronic surveillance of foreign nationals located abroad under a reduced government burden compared with traditional electronic foreign intelligence surveillance. *Compare* 50 U.S.C. § 1805 (2012) (amended 2018) (requiring "probable cause to believe . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power"), *with* 50 U.S.C. § 1881a (requiring that surveillance not intentionally target people in the United States or United States nationals but not requiring any showing that the surveillance target is a foreign power or agent of a foreign power).

The Court then held that the plaintiffs' theory of injury was too speculative to constitute a "certainly impending" injury. *Id.* at 410. The plaintiffs had not alleged that any of their communications had yet been intercepted. *Id.* at 411. The Court characterized their alleged injury as instead resting on a series of inferences, including that:

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 410. The Court declined to speculate about what it described as independent choices by the government about whom to target for surveillance and what basis to invoke for such targeting, or about whether the Foreign Intelligence Surveillance Court would approve any such surveillance. *Id.* at 412–13. The plaintiffs' multi-link chain of inferences was thus "too speculative" to constitute a cognizable injury in fact. *Id.* at 401.

Unlike in *Clapper*, the plaintiffs' alleged injury in *Krottner* did not require a speculative multi-link chain of inferences. *See Krottner*, 628 F.3d at 1143. The *Krottner* laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that *Krottner* collectively treats as "identity theft." *Id.* at 1142. Moreover, *Clapper*'s standing analysis was "especially rigorous" because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional. *Clapper*, 568 U.S. at 408 (quoting *Raines v. Byrd*, 521 U.S. 811, 819 (1997)). *Krottner* presented no such national security or separation of powers concerns.

And although the Supreme Court focused in *Clapper* on whether the injury was "certainly impending," it acknowledged that other cases had focused on whether there was a "substantial risk" of injury.[5] *Id.* at 414 & n.5. Since *Clapper*, the Court reemphasized in *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (2014), that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" *Id.* at 2341 (quoting *Clapper*, 568 U.S. at 414 & n.5) (internal quotation marks omitted).

[5] The Court noted that the plaintiffs in *Clapper* had not alleged a substantial risk because their theory of injury relied on too many inferences. *Clapper*, 568 U.S. at 414 n.5.

For all these reasons, we hold that *Krottner* is not clearly irreconcilable with *Clapper* and thus remains binding.[6] *See Miller*, 335 F.3d at 900.

B.

We also conclude that *Krottner* controls the result here. In *Krottner*, we held that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." 628 F.3d at 1143. The threat would have been "far less credible," we explained, "if no laptop had been stolen, and [they] had sued based on the risk that it would be stolen

[6] Our conclusion that *Krottner* is not clearly irreconcilable with *Clapper* is consistent with post-*Clapper* decisions in our sister circuits holding that data breaches in which hackers targeted PII created a risk of harm sufficient to support standing. For example, the D.C. Circuit held in *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018), that "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs [who were victims of a data breach] will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629; *see also Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's 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."). The Eighth Circuit did hold in *In re SuperValu, Inc., Customer Data Security Breach Litigation*, 870 F.3d 763 (8th Cir. 2017), that allegations of the theft of credit card information were insufficient to support standing. *Id.* at 771–72. But no other PII, such as addresses, telephone numbers, or passwords, was stolen in that case. *See id.* at 766, 770. The Eighth Circuit acknowledged cases like *Attias* and *Remijas* but opined that standing questions in data breach cases "ultimately turn[] on the substance of the allegations before each court"—particularly, the types of data allegedly stolen. *Id.* at 769.

at some point in the future." *Id.* But the sensitivity of the personal information, combined with its theft, led us to conclude that the plaintiffs had adequately alleged an injury in fact supporting standing. *Id.* The sensitivity of the stolen data in this case is sufficiently similar to that in *Krottner* to require the same conclusion here.

Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of "phishing" and "pharming," which are ways for hackers to exploit information they already have to get even more PII. Plaintiffs also allege that their credit card numbers were within the information taken in the breach—which was not true in *Krottner*.[7] And Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft. *See* 15 U.S.C. § 1681c(g) (2012). Although there is no allegation in this case that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used "the same or a similar password."[8]

[7] Plaintiffs include in the Complaint some emails sent to Zappos from other customers saying that their credit cards were fraudulently used following the breach.

[8] We use the terms "identity fraud" and "identity theft" in accordance with the GAO definition Plaintiffs rely on in the Complaint. *See supra* note 3 and accompanying text.

Indeed, the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos specifically alleged that they suffered financial losses because of the Zappos data breach (which is why the district court held that they had standing). Although those plaintiffs' claims are not at issue in this appeal, their alleged harm undermines Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft. In addition, two plaintiffs whose claims are at issue in this appeal say that the hackers took over their AOL accounts and sent advertisements to people in their address books.[9] Though not a financial harm, these alleged attacks further support Plaintiffs' contention that the hackers accessed information that could be used to help commit identity fraud or identity theft. We thus conclude that Plaintiffs have sufficiently alleged an injury in fact under *Krottner*.

Zappos contends that even if the stolen data was as sensitive as that in *Krottner*, too much time has passed since the breach for any harm to be imminent. Zappos is mistaken. Our jurisdiction "depends upon the state of things at the time of the action brought."[10] *Mollan v. Torrance*, 22 U.S. 537, 539 (1824). The initial complaint against Zappos was filed on the same day that Zappos provided notice of the breach. Other Plaintiffs' complaints were filed soon thereafter. We

[9] The district court held that these plaintiffs nonetheless lacked standing because they had not suffered "additional misuse" or "actual damages" from the data breach.

[10] Consistent with this principle, *Krottner* did not discuss the two-year gap between the breach and the appeal, focusing instead on the sensitivity of the stolen information. *See* 628 F.3d at 1143.

therefore assess Plaintiffs' standing as of January 2012, not as of the present.[11]

Plaintiffs also specifically allege that "[a] person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years." And "it may take some time for the victim to become aware of the theft."

Assessing the sum of their allegations in light of *Krottner*, Plaintiffs have sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft.[12]

---

[11] Of course, as litigation proceeds beyond the pleadings stage, the Complaint's allegations will not sustain Plaintiffs' standing on their own. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach element [of Article III standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation."). In opposing a motion for summary judgment, for example, Plaintiffs would need to come forward with evidence to support standing. *See id.* But the passage of time does not change the relevant moment as to which Plaintiffs must establish that they had standing or heighten Plaintiffs' burden in opposing the motion to dismiss. *See id.*; *Mollan*, 22 U.S. at 539. A case may also, of course, become moot as time progresses. But there is no reason to doubt that Plaintiffs still have a live controversy against Zappos here. *Cf. Z Channel Ltd. P'ship v. Home Box Office, Inc.*, 931 F.2d 1338, 1341 (9th Cir. 1991) ("If [a plaintiff] is entitled to collect damages in the event that it succeeds on the merits, the case does not become moot even though declaratory and injunctive relief are no longer of any use.").

[12] This conclusion is consistent with the Fourth Circuit's decision in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017). The plaintiffs in *Beck*, patients with personal data on a laptop stolen from a hospital, did not allege that the "thief intentionally targeted the personal information compromised

C.

The remaining Article III standing requirements are also satisfied. Plaintiffs sufficiently allege that the risk of future harm they face is "'fairly traceable' to the conduct being challenged"—here, Zappos's failure to prevent the breach. *Wittman v. Personhuballah*, 136 S. Ct. 1732, 1736 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)).

That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages. As the Seventh Circuit recognized in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), that "some other store *might* [also] have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue" for the breach in

---

in the data breaches." *Id.* at 274. The Fourth Circuit held that the absence of such an allegation "render[ed] their contention of an enhanced risk of future identity theft too speculative." *Id.* Here, by contrast, Plaintiffs allege that hackers specifically targeted their PII on Zappos's servers. It is true that in *Beck* the Fourth Circuit opined that "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Id.* at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016), and citing *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015)). But the time since the data breach appears to have mattered in *Beck* because the court concluded that the plaintiffs lacked standing after the breach in the first place, so it made sense to consider whether any subsequent events suggested a greater injury than was initially apparent. *See id.* at 274.

question.[13] *Id.* at 696; *cf. Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring in the judgment) ("[I]n multiple causation cases, . . . the common law of torts has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." (citing *Summers v. Tice*, 199 P.2d 1, 3–4 (Cal. 1948))), *superseded on other grounds by* 42 U.S.C. § 2000e-2(m) (2012).

The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. *See Lujan*, 504 U.S. at 561. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages. *See Remijas*, 794 F.3d at 696–97. And at least some of their requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to

[13] *Clapper* is not to the contrary. In *Clapper*, the Supreme Court held that, even assuming the plaintiffs were going to be surveilled, any future surveillance could not be traced to the challenged statute because the risk of being surveilled did not increase with the addition of the new statutory tool. 568 U.S. at 413 ("[B]ecause respondents can only speculate as to whether any (asserted) interception would be under § 1881a or some other authority, they cannot satisfy the 'fairly traceable' requirement."). There were many surveillance options, all of which were in the hands of one actor: the government. Thus, a plaintiff's risk of surveillance hinged on whether the government chose to surveil him in the first place. In contrast, with each new hack comes a new hacker, each of whom independently could choose to use the data to commit identity theft. This means that each hacking incident adds to the overall risk of identity theft. And again, as explained above, the key injury recognized in *Krottner* is the risk of being subject to identity theft, not actual identity theft.

monitor their credit and the like.[14] *See Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 154–55 (2010).

IV.

For the foregoing reasons, we **REVERSE** the district court's judgment as to Plaintiffs' standing and **REMAND**.

[14] Plaintiffs need only one viable basis for standing. *See Douglas Cty. v. Babbitt*, 48 F.3d 1495, 1500 (9th Cir. 1995). Because Plaintiffs sufficiently allege standing from the risk of future identity theft, we do not reach their other asserted bases for standing.

EXHIBIT 2

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION, THERESA STEVENS; KRISTIN O'BRIEN; TERRI WADSWORTH; DAHLIA HABASHY; PATTI HASNER; SHARI SIMON; STEPHANIE PRIERA; KATHRYN VORHOFF; DENISE RELETHFORD; ROBERT REE, *Plaintiffs-Appellants*, v. ZAPPOS.COM., INC., *Defendant-Appellee.*	No. 16-16860 D.C. No. 3:12-cv-00325-RCJ-VPC ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the District of Nevada
Robert Clive Jones, Senior District Judge, Presiding

Argued and Submitted December 5, 2017
San Francisco, California

Filed March 8, 2018
Amended April 20, 2018

Before: John B. Owens and Michelle T. Friedland, Circuit Judges, and Elaine E. Bucklo,* District Judge.

Order;
Opinion by Judge Friedland

SUMMARY**

Article III Standing

The panel amended the opinion filed on March 8, 2018; and reversed the district court's dismissal, for lack of Article III standing, of plaintiffs' claims alleging that they were harmed by hacking of their accounts at the online retailer Zappos.com.

The panel held that under *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), plaintiffs sufficiently alleged standing based on the risk of identity theft. The panel rejected Zappos's argument that *Krottner* was no longer good law after *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). The panel held that plaintiffs sufficiently alleged an injury in fact under *Krottner*, based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft. The panel further held that plaintiffs sufficiently alleged that the risk of future harm they faced was "fairly traceable" to the conduct being challenged; and

* The Honorable Elaine E. Bucklo, United States District Judge for the Northern District of Illinois, sitting by designation.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

the risk from the injury of identity theft was also redressable by relief that could be obtained through this litigation.

The panel addressed an issue raised by sealed briefing in a concurrently filed memorandum disposition.

COUNSEL

Douglas Gregory Blankinship (argued), Finkelstein Blankinship Frei-Pearson and Garber LLP, White Plains, New York; David C. O'Mara, The O'Mara Law Firm P.C., Reno, Nevada; Ben Barnow, Barnow and Associates P.C., Chicago, Illinois; Richard L. Coffman, The Coffman Law Firm, Beaumont, Texas; Marc L. Godino, Glancy Binkow & Goldberg LLP, Los Angeles, California; for Plaintiffs-Appellants.

Stephen J. Newman (argued), David W. Moon, Brian C. Frontino, and Julia B. Strickland, Stroock & Stroock & Lavan LLP, Los Angeles, California; Robert McCoy, Kaempfer Crowell, Las Vegas, Nevada; for Defendant-Appellee.

ORDER

The opinion filed on March 8, 2018, and appearing at 884 F.3d 893, is amended as follows. On page 899:

Replace <Zappos is mistaken . . . the present> with <Zappos initially contended on appeal that the relevant time at which to assess standing was the present. But it could not offer any support for that contention. After our opinion was initially filed, Zappos sought rehearing on this issue, urging us to read *Rockwell International Corp. v. United States*, 549 U.S. 457, 473 (2007), and *Northstar Financial Advisors Inc. v. Schwab Investments*, 779 F.3d 1036, 1044 (9th Cir. 2015), to require that we assess standing at the time Plaintiffs filed their operative Third Amended Complaint, rather than their original Complaints. But whether we look at the original Complaints or Plaintiffs' Third Amended Complaint, the allegations about the increased risk of harm Plaintiffs face are relevantly the same—in the Complaints, Plaintiffs allege that the Zappos data breach places them at imminent risk of identity theft. Zappos argues that this allegation is implausible, but it does so by relying on facts outside the Complaints (or contentions about the absence of certain facts), which makes its argument one that may be appropriate for summary judgment but not one that may support a facial challenge to standing at the motion to dismiss stage>.

Following <rather than their original Complaints.> in the above replacement text, insert a footnote <Zappos's reliance on these cases is also unconvincing, as these cases do not actually address whether standing is measured at the time of an initial complaint or at the time of an amended complaint, as opposed to whether the allegations in an amended complaint may sometimes be considered in evaluating whether there was standing at the time the case was

originally filed or whether an amended complaint may be considered a supplemental pleading under Federal Rule of Civil Procedure 15(d).>.

Following <imminent risk of identity theft.> in the above replacement text, insert a footnote <Plaintiff Robert Ree does not clearly allege a risk of future identity theft. But even assuming Ree would not have had standing on his own based on his original Complaint, only one Plaintiff needs to have standing for a class action to proceed. *See Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (en banc).>.

In the current footnote 11, delete <; *Mollan*, 22 U.S. at 539.>.

With these amendments, the panel has unanimously voted to deny appellee's petition for rehearing. Judge Owens and Judge Friedland have voted to deny the petition for rehearing en banc. Judge Bucklo recommends denial of the petition for rehearing en banc. The full court has been advised of the petition for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petitions for rehearing and rehearing en banc are **DENIED**. No further petitions shall be entertained.

OPINION

FRIEDLAND, Circuit Judge:

In January 2012, hackers breached the servers of online retailer Zappos.com, Inc. ("Zappos") and allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers. Several of those customers filed putative class actions in federal courts across the country, asserting that Zappos had not adequately protected their personal information. Their lawsuits were consolidated for pretrial proceedings.

Although some of the plaintiffs alleged that the hackers used stolen information about them to conduct subsequent financial transactions, the plaintiffs who are the focus of this appeal ("Plaintiffs") did not. This appeal concerns claims based on the hacking incident itself, not any subsequent illegal activity.

The district court dismissed Plaintiffs' claims for lack of Article III standing. In this appeal, Plaintiffs contend that the district court erred in doing so, and they press several potential bases for standing, including that the Zappos data breach put them at risk of identity theft.

We addressed standing in an analogous context in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). There, we held that employees of Starbucks had standing to sue the company based on the risk of identity theft they faced after a company laptop containing their personal information was stolen. *Id.* at 1140, 1143. We reject Zappos's argument that *Krottner* is no longer good law after *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), and hold that, under

Krottner, Plaintiffs have sufficiently alleged standing based on the risk of identity theft.[1]

I.

When they bought merchandise on Zappos's website, customers provided personal identifying information ("PII"), including their names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information. Sometime before January 16, 2012, hackers targeted Zappos's servers, stealing the PII of more than 24 million of its customers, including their full credit card numbers.[2] On January 16, Zappos sent an email to its customers, notifying them of the theft of their PII. The company recommended "that they reset their Zappos.com account passwords and change the passwords 'on any other web site where [they] use the same or a similar password.'" Some customers responded almost immediately by filing putative class actions in federal district courts across the country.

[1] We address an issue raised by sealed briefing in a concurrently filed memorandum disposition.

[2] Although Zappos asserts in its briefs that the hackers stole only the last four digits of customers' credit card numbers, it has presented its arguments as a facial, not a factual, attack on standing. *See Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004) (distinguishing facial from factual attacks on standing). Where, as here, "a defendant in its motion to dismiss under Federal Rule of Civil Procedure 12(b)(1) asserts that the allegations in the complaint are insufficient to establish subject matter jurisdiction as a matter of law (to be distinguished from a claim that the allegations on which jurisdiction depends are not true as a matter of fact), we take the allegations in the plaintiff's complaint as true." *Whisnant v. United States*, 400 F.3d 1177, 1179 (9th Cir. 2005).

In these suits, Plaintiffs alleged an "imminent" risk of identity theft or fraud from the Zappos breach. Relying on definitions from the United States Government Accountability Office ("GAO"), they characterized "identity theft" and "identity fraud" as "encompassing various types of criminal activities, such as when PII is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud."[3]

The Judicial Panel on Multidistrict Litigation transferred several putative class action lawsuits alleging harms from the Zappos data breach to the District of Nevada for pretrial proceedings. After several years of pleadings-stage litigation, including a hiatus for mediation, the district court granted in part and denied in part Zappos's motion to dismiss the Third Amended Consolidated Complaint ("Complaint") and granted Zappos's motion to strike the Complaint's class allegations. The court distinguished between two groups of plaintiffs: (1) plaintiffs named only in the Third Amended Complaint who alleged that they had already suffered financial losses from identity theft caused by Zappos's breach, and (2) plaintiffs named in earlier complaints who did not allege having already suffered financial losses from identity theft.

[3] Plaintiffs did not provide a precise cite but appear to be referring to the description of identity theft in a report entitled *Personal Information*, which explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." U.S. Gov't Accountability Office, GAO-07-737, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* 2 (2007).

The district court ruled that the first group of plaintiffs had Article III standing because they alleged "that actual fraud occurred as a direct result of the breach." But the court ruled that the second group of plaintiffs (again, here referred to as "Plaintiffs") lacked Article III standing and dismissed their claims without leave to amend because Plaintiffs had "failed to allege instances of actual identity theft or fraud." The parties then agreed to dismiss all remaining claims with prejudice, and Plaintiffs appealed.

II.

We review the district court's standing determination de novo. *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). To have Article III standing,

> a plaintiff must show (1) it 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. (TOC), Inc., 528 U.S. 167, 180–81 (2000); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). A plaintiff threatened with future injury has standing to sue "if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013)) (internal quotation marks omitted).

III.

We addressed the Article III standing of victims of data theft in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). In *Krottner*, a thief stole a laptop containing "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees." *Id.* at 1140. "Starbucks sent a letter to . . . affected employees alerting them to the theft and stating that Starbucks had no indication that the private information ha[d] been misused," but advising them to "monitor [their] financial accounts carefully for suspicious activity and take appropriate steps to protect [themselves] against potential identity theft." *Id.* at 1140–41 (internal quotation marks omitted). Some employees sued, and the only harm that most alleged was an "increased risk of future identity theft." *Id.* at 1142. We determined this was sufficient for Article III standing, holding that the plaintiffs had "alleged a credible threat of real and immediate harm" because the laptop with their PII had been stolen. *Id.* at 1143.

A.

Before analyzing whether *Krottner* controls this case, we must determine whether *Krottner* remains good law after the Supreme Court's more recent decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), which addressed a question of standing based on the risk of future harm.

As a three-judge panel, we are bound by opinions of our court on issues of federal law unless those opinions are "clearly irreconcilable" with a later decision by the Supreme Court or our court sitting en banc. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). This is the first case

to require us to consider whether *Clapper* and *Krottner* are clearly irreconcilable, and we conclude that they are not.

The plaintiffs in *Clapper* challenged surveillance procedures authorized by the Foreign Intelligence Surveillance Act of 1978—specifically, in 50 U.S.C. § 1881a (2012) (amended 2018).[4] *Clapper*, 568 U.S. at 401. The plaintiffs, who were "attorneys and human rights, labor, legal, and media organizations whose work allegedly require[d] them to engage in sensitive and sometimes privileged telephone and e-mail communications with . . . individuals located abroad," sued for declaratory relief to invalidate § 1881a and an injunction against surveillance conducted pursuant to that section. *Id.* at 401, 406. The plaintiffs argued that they had Article III standing to challenge § 1881a "because there [was] an objectively reasonable likelihood that their communications [would] be acquired under § 1881a at some point in the future." *Id.* at 401. The Supreme Court rejected this basis for standing, explaining that "an objectively reasonable likelihood" of injury was insufficient, and that the alleged harm needed to "satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

[4] 50 U.S.C. § 1881a authorizes electronic surveillance of foreign nationals located abroad under a reduced government burden compared with traditional electronic foreign intelligence surveillance. *Compare* 50 U.S.C. § 1805 (2012) (amended 2018) (requiring "probable cause to believe . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power"), *with* 50 U.S.C. § 1881a (requiring that surveillance not intentionally target people in the United States or United States nationals but not requiring any showing that the surveillance target is a foreign power or agent of a foreign power).

The Court then held that the plaintiffs' theory of injury was too speculative to constitute a "certainly impending" injury. *Id.* at 410. The plaintiffs had not alleged that any of their communications had yet been intercepted. *Id.* at 411. The Court characterized their alleged injury as instead resting on a series of inferences, including that:

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 410. The Court declined to speculate about what it described as independent choices by the government about whom to target for surveillance and what basis to invoke for such targeting, or about whether the Foreign Intelligence Surveillance Court would approve any such surveillance. *Id.* at 412–13. The plaintiffs' multi-link chain of inferences was thus "too speculative" to constitute a cognizable injury in fact. *Id.* at 401.

Unlike in *Clapper*, the plaintiffs' alleged injury in *Krottner* did not require a speculative multi-link chain of inferences. *See Krottner*, 628 F.3d at 1143. The *Krottner* laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that *Krottner* collectively treats as "identity theft." *Id.* at 1142. Moreover, *Clapper*'s standing analysis was "especially rigorous" because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional. *Clapper*, 568 U.S. at 408 (quoting *Raines v. Byrd*, 521 U.S. 811, 819 (1997)). *Krottner* presented no such national security or separation of powers concerns.

And although the Supreme Court focused in *Clapper* on whether the injury was "certainly impending," it acknowledged that other cases had focused on whether there was a "substantial risk" of injury.[5] *Id.* at 414 & n.5. Since *Clapper*, the Court reemphasized in *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (2014), that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk that the harm will occur.'" *Id.* at 2341 (quoting *Clapper*, 568 U.S. at 414 & n.5) (internal quotation marks omitted).

[5] The Court noted that the plaintiffs in *Clapper* had not alleged a substantial risk because their theory of injury relied on too many inferences. *Clapper*, 568 U.S. at 414 n.5.

For all these reasons, we hold that *Krottner* is not clearly irreconcilable with *Clapper* and thus remains binding.[6] *See Miller*, 335 F.3d at 900.

B.

We also conclude that *Krottner* controls the result here. In *Krottner*, we held that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." 628 F.3d at 1143. The threat would have been "far less credible," we explained, "if no laptop had been stolen, and [they] had sued based on the risk that it would be stolen

[6] Our conclusion that *Krottner* is not clearly irreconcilable with *Clapper* is consistent with post-*Clapper* decisions in our sister circuits holding that data breaches in which hackers targeted PII created a risk of harm sufficient to support standing. For example, the D.C. Circuit held in *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018), that "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs [who were victims of a data breach] will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629; *see also Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's 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."). The Eighth Circuit did hold in *In re SuperValu, Inc., Customer Data Security Breach Litigation*, 870 F.3d 763 (8th Cir. 2017), that allegations of the theft of credit card information were insufficient to support standing. *Id.* at 771–72. But no other PII, such as addresses, telephone numbers, or passwords, was stolen in that case. *See id.* at 766, 770. The Eighth Circuit acknowledged cases like *Attias* and *Remijas* but opined that standing questions in data breach cases "ultimately turn[] on the substance of the allegations before each court"—particularly, the types of data allegedly stolen. *Id.* at 769.

at some point in the future." *Id.* But the sensitivity of the personal information, combined with its theft, led us to conclude that the plaintiffs had adequately alleged an injury in fact supporting standing. *Id.* The sensitivity of the stolen data in this case is sufficiently similar to that in *Krottner* to require the same conclusion here.

Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of "phishing" and "pharming," which are ways for hackers to exploit information they already have to get even more PII. Plaintiffs also allege that their credit card numbers were within the information taken in the breach—which was not true in *Krottner*.[7] And Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft. *See* 15 U.S.C. § 1681c(g) (2012). Although there is no allegation in this case that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used "the same or a similar password."[8]

[7] Plaintiffs include in the Complaint some emails sent to Zappos from other customers saying that their credit cards were fraudulently used following the breach.

[8] We use the terms "identity fraud" and "identity theft" in accordance with the GAO definition Plaintiffs rely on in the Complaint. *See supra* note 3 and accompanying text.

Indeed, the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos specifically alleged that they suffered financial losses because of the Zappos data breach (which is why the district court held that they had standing). Although those plaintiffs' claims are not at issue in this appeal, their alleged harm undermines Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft. In addition, two plaintiffs whose claims are at issue in this appeal say that the hackers took over their AOL accounts and sent advertisements to people in their address books.[9] Though not a financial harm, these alleged attacks further support Plaintiffs' contention that the hackers accessed information that could be used to help commit identity fraud or identity theft. We thus conclude that Plaintiffs have sufficiently alleged an injury in fact under *Krottner*.

Zappos contends that even if the stolen data was as sensitive as that in *Krottner*, too much time has passed since the breach for any harm to be imminent. Zappos initially contended on appeal that the relevant time at which to assess standing was the present. But it could not offer any support for that contention. After our opinion was initially filed, Zappos sought rehearing on this issue, urging us to read *Rockwell International Corp. v. United States*, 549 U.S. 457, 473 (2007), and *Northstar Financial Advisors Inc. v. Schwab Investments*, 779 F.3d 1036, 1044 (9th Cir. 2015), to require that we assess standing at the time Plaintiffs filed their operative Third Amended Complaint, rather than their

[9] The district court held that these plaintiffs nonetheless lacked standing because they had not suffered "additional misuse" or "actual damages" from the data breach.

original Complaints.[10] But whether we look at the original Complaints or Plaintiffs' Third Amended Complaint, the allegations about the increased risk of harm Plaintiffs face are relevantly the same—in the Complaints, Plaintiffs allege that the Zappos data breach places them at imminent risk of identity theft.[11] Zappos argues that this allegation is implausible, but it does so by relying on facts outside the Complaints (or contentions about the absence of certain facts), which makes its argument one that may be appropriate for summary judgment but not one that may support a facial challenge to standing at the motion to dismiss stage[12]

[10] Zappos's reliance on these cases is also unconvincing, as these cases do not actually address whether standing is measured at the time of an initial complaint or at the time of an amended complaint, as opposed to whether the allegations in an amended complaint may sometimes be considered in evaluating whether there was standing at the time the case was originally filed or whether an amended complaint may be considered a supplemental pleading under Federal Rule of Civil Procedure 15(d).

[11] Plaintiff Robert Ree does not clearly allege a risk of future identity theft. But even assuming Ree would not have had standing on his own based on his original Complaint, only one Plaintiff needs to have standing for a class action to proceed. *See Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (en banc).

[12] Of course, as litigation proceeds beyond the pleadings stage, the Complaint's allegations will not sustain Plaintiffs' standing on their own. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach element [of Article III standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation."). In opposing a motion for summary judgment, for example, Plaintiffs would need to come forward with evidence to support standing. *See id.* But the passage of time does not change the relevant moment as

Plaintiffs also specifically allege that "[a] person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years." And "it may take some time for the victim to become aware of the theft."

Assessing the sum of their allegations in light of *Krottner*, Plaintiffs have sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft.[13]

---

to which Plaintiffs must establish that they had standing or heighten Plaintiffs' burden in opposing the motion to dismiss. *See id*. A case may also, of course, become moot as time progresses. But there is no reason to doubt that Plaintiffs still have a live controversy against Zappos here. *Cf. Z Channel Ltd. P'ship v. Home Box Office, Inc.*, 931 F.2d 1338, 1341 (9th Cir. 1991) ("If [a plaintiff] is entitled to collect damages in the event that it succeeds on the merits, the case does not become moot even though declaratory and injunctive relief are no longer of any use.").

[13] This conclusion is consistent with the Fourth Circuit's decision in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017). The plaintiffs in *Beck*, patients with personal data on a laptop stolen from a hospital, did not allege that the "thief intentionally targeted the personal information compromised in the data breaches." *Id.* at 274. The Fourth Circuit held that the absence of such an allegation "render[ed] their contention of an enhanced risk of future identity theft too speculative." *Id.* Here, by contrast, Plaintiffs allege that hackers specifically targeted their PII on Zappos's servers. It is true that in *Beck* the Fourth Circuit opined that "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Id.* at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016), and citing *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015)). But the time since the data breach appears to have mattered in *Beck* because the court concluded that the plaintiffs lacked standing after the breach in the first place, so it made sense to consider whether any

C.

The remaining Article III standing requirements are also satisfied. Plaintiffs sufficiently allege that the risk of future harm they face is "'fairly traceable' to the conduct being challenged"—here, Zappos's failure to prevent the breach. *Wittman v. Personhuballah*, 136 S. Ct. 1732, 1736 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)).

That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages. As the Seventh Circuit recognized in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), that "some other store *might* [also] have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue" for the breach in question.[14] *Id.* at 696; *cf. Price Waterhouse v. Hopkins*,

subsequent events suggested a greater injury than was initially apparent. *See id.* at 274.

[14] *Clapper* is not to the contrary. In *Clapper*, the Supreme Court held that, even assuming the plaintiffs were going to be surveilled, any future surveillance could not be traced to the challenged statute because the risk of being surveilled did not increase with the addition of the new statutory tool. 568 U.S. at 413 ("[B]ecause respondents can only speculate as to whether any (asserted) interception would be under § 1881a or some other authority, they cannot satisfy the 'fairly traceable' requirement."). There were many surveillance options, all of which were in the hands of one actor: the government. Thus, a plaintiff's risk of surveillance hinged on whether the government chose to surveil him in the first place. In contrast, with each new hack comes a new hacker, each of whom independently could choose to use the data to commit identity

490 U.S. 228, 263 (1989) (O'Connor, J., concurring in the judgment) ("[I]n multiple causation cases, . . . the common law of torts has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." (citing *Summers v. Tice*, 199 P.2d 1, 3–4 (Cal. 1948))), *superseded on other grounds by* 42 U.S.C. § 2000e-2(m) (2012).

The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. *See Lujan*, 504 U.S. at 561. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages. *See Remijas*, 794 F.3d at 696–97. And at least some of their requested injunctive relief would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit and the like.[15] *See Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 154–55 (2010).

IV.

For the foregoing reasons, we **REVERSE** the district court's judgment as to Plaintiffs' standing and **REMAND**.

---

theft. This means that each hacking incident adds to the overall risk of identity theft. And again, as explained above, the key injury recognized in *Krottner* is the risk of being subject to identity theft, not actual identity theft.

[15] Plaintiffs need only one viable basis for standing. *See Douglas Cty. v. Babbitt*, 48 F.3d 1495, 1500 (9th Cir. 1995). Because Plaintiffs sufficiently allege standing from the risk of future identity theft, we do not reach their other asserted bases for standing.