APPENDIX

TABLE OF APPENDICES

Appendix A

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 16-16860

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.

Appeal from the United States District Court
for the District of Nevada

Argued and Submitted December 5, 2017
San Francisco, California

Filed March 8, 2018
Amended April 20, 2018

ORDER AND AMENDED OPINION

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

[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).

password.'" Some customers responded almost immediately by filing putative class actions in federal district courts across the country.

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:

---

[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).

(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.

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

[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).

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)).

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

[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.

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).

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.

---

[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.

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 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

[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.

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]

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*.

---

[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.

[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.

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 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

---

[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).

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]

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

---

[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 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.").

in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft.[13]

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

---

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

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*, 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).

---

[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 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.

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.

---

[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.

Appendix B

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 16-16860

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.

Appeal from the United States District Court
for the District of Nevada

Filed: May 8, 2018

ORDER

Before: Owens and Friedland, Circuit Judges, and Bucklo,* District Judge.

Appellee Zappos.com, Inc.'s motion to stay issuance of the mandate pending application for writ of certiorari is granted. Fed. R. App. P. 41(d)(2)(A).

The mandate is stayed for a period not to exceed 90 days pending the filing of the petition for a writ of certiorari in the Supreme Court. If, within that period, the Clerk of the Supreme Court advises the Clerk of this Court that a petition for certiorari has been filed, the stay shall continue until final disposition of the matter by the Supreme Court.

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

Appendix C

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 16-16860

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.

Appeal from the United States District Court
for the District of Nevada

Filed: July 6, 2018

ORDER

Before: Owens and Friedland, Circuit Judges, and Bucklo,* District Judge.

Zappos.com, Inc.'s motion to extend the stay of issuance of the mandate pending application for a writ of certiorari is granted. Fed. R. App. P. 41(d)(2)(B).

The stay is extended until August 20, 2018, pending the filing of the petition for a writ of certiorari in the Supreme Court. If, within that period, the Clerk of the Supreme Court advises the Clerk of this Court that a petition for certiorari has been filed, the stay shall continue until final disposition of the matter by the Supreme Court.

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

Appendix D

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEVADA

No. 3:12-cv-00325
MDL No. 2357

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION,

---

Filed: September 13, 2016

STIPULATION AND ORDER GRANTING DISMISSAL WITH PREJUDICE AS TO ALL CLAIMS FOR PLAINTIFFS

WHEREAS, the history of this litigation is protracted.

WHEREAS, on September 9, 2013, the Court entered an order granting in part and denying in part Defendant Zappos, Inc.'s ("Defendant") motion to dismiss. Dkt. No. 114.

WHEREAS, on March 27, 2015, the Court entered an Order denying Plaintiffs' Motion to Enforce Settlement. Dkt. No. 227.

WHEREAS, on June 1, 2015, the Court entered an Order dismissing Plaintiffs' claims without prejudice. Dkt. No. 235.

WHEREAS, on May 6, 2016, the Court entered an Order dismissing most of Plaintiffs' claims with

prejudice and striking Plaintiffs' class allegations as they were pleaded. Dkt. No. 279.

WHEREAS, on August 29, 2016, the Court entered an Order granting in part and denying in part Plaintiffs' Motion for Reconsideration. Dkt. No. 287.

WHEREAS, all Plaintiffs now desire to seek appellate review, and they seek to do so without delay rather than continuing to litigate the few claims potentially remaining before this Court to finality;

WHEREAS, all parties agree to waive any claims to costs and attorney's fees as a result of Plaintiffs' dismissals of their claims;

WHEREAS, Plaintiffs and Defendant have met and conferred and have agreed pursuant to Fed. R. Civ. P. 41(a)(1) to stipulate to a voluntary dismissal with prejudice of any and all remaining claims in this action for the purpose of terminating this Court's jurisdiction over this case so that all Plaintiffs may appeal to the United States Court of Appeals for the Ninth Circuit;

IT IS HEREBY STIPULATED BY AND BETWEEN Plaintiffs and Defendant, through their respective counsel of record, that any and all remaining claims shall be voluntarily dismissed with prejudice pursuant to a final Order, the nature of which is described in 28 U.S.C. § 1291, with each party to bear its own attorneys' fees and costs.

IS IS SO STIPULATED.

IT IS SO ORDERED this 13th day of September, 2016.

[handwritten: signature]
Robert C. Jones

Appendix E

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEVADA

No. 3:12-cv-00325
MDL No. 2357

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION,

---

Filed: May 6, 2016

ORDER

This multidistrict litigation case arises out of a security breach of Zappos.com's customer data. Pending before the Court is a Motion to Dismiss (ECF No. 254), filed by Amazon.com, Inc. doing business as Zappos.com ("Zappos"). Also pending are Zappos's Motion to Strike (ECF No. 255), three Motions to Seal (ECF Nos. 244, 248, 266), and a Motion for Leave to File Excess Pages (ECF No. 275).

I. FACTS AND PROCEDURAL HISTORY

On January 15, 2012, a hacker or group of hackers targeted Zappos's servers located in Kentucky and Nevada. The servers contained the personal identifying information ("PII") of approximately 24 million Zappos's customers. On January 16, 2012, Zappos sent an email to its customers notifying them that its servers had been breached and that data had been stolen, including customers' names, account

numbers, passwords, email addresses, billing and shipping addresses, phone numbers, and the last four digits of their credit cards used to make purchases. Shortly thereafter, a number of lawsuits were filed against Zappos seeking damages.

On June 14, 2012, the U.S. Judicial Panel on Multidistrict Litigation ("JPML") granted Zappos's motion to create the present case pursuant to 28 U.S.C. § 1407, transferring six extra-district actions to this District, consolidating them with three actions from this District, and assigning the consolidated case to this Court. (Transfer Order, ECF No. 1). Zappos moved to compel arbitration and stay the case. While that motion was pending, the JPML transferred an additional action to be consolidated with the instant case. (Conditional Transfer Order, ECF No. 5). The Court denied the motion to compel arbitration because the arbitration contract was "browsewrap" not requiring any objective manifestation of assent (as opposed to a "clickwrap" agreement), and there was no evidence that Plaintiffs had knowledge of the offer such that assent could be implied merely by use of the website. (*See* Order, 7-10, ECF No. 21).

Plaintiffs then amended their pleadings into two separate consolidated class action complaints, and Zappos filed a motion to dismiss the amended complaints for lack of standing and for failure to state a claim. (ECF No. 62). On September 9, 2013, the Court granted in part and denied in part Zappos's motion. (ECF No. 114). Thereafter, Plaintiffs Preira, Ree, Simon, Hasner, Habashy, and Nobles ("the Preira Plaintiffs") filed their Second Amended Consolidated Complaint (the "Preira SAC"). (ECF No. 118). And

Plaintiffs Stevens, Penson, Elliot, Brown, Seal, Relethford, and Braxton (the "Stevens Plaintiffs") filed their Second Amended Consolidated Class Action Complaint (the "Stevens SAC"). (ECF No. 119).

On November 4, 2013, Zappos moved to dismiss the Preira SAC and the Stevens SAC. (ECF No. 122). While that motion was pending, the parties engaged in mediation in an attempt to reach a settlement. The parties stipulated to stay the proceedings various times, each time representing to the Court that settlement negotiations were progressing. (*See* ECF Nos. 192, 196, 201). Despite the progress made during mediation as to class-wide relief, a final agreement could not be reached between the parties due to a disagreement over attorneys' fees. However, on December 4, 2014, Plaintiffs filed a motion to enforce a supposed settlement, which the Court denied. (ECF No. 227). Zappos then renewed its previous dismissal arguments. The Court granted the motion to dismiss, holding that Plaintiffs have no standing because, among other reasons, they failed to allege a threat of imminent future harm or instances of actual identity theft or fraud. (ECF No. 235). The Court dismissed the complaints without prejudice, granting Plaintiffs leave to amend their complaints to allege instances of actual identity theft or fraud.

Following the Court's order, the Preira Plaintiffs and the Stevens Plaintiffs ("Prior Plaintiffs") filed a consolidated Third Amended Complaint ("TAC"). (ECF Nos. 245, 246). In the TAC, two new Plaintiffs—Kristin O'Brien and Terri Wadsworth ("New Plaintiffs")—were added to the case. Once again, Zappos moves the Court to dismiss the case or,

alternatively, to strike the class allegations in the TAC.

II. LEGAL STANDARDS

"Lack of standing is a defect in subject-matter jurisdiction and may properly be challenged under Rule 12(b)(1)." *Wright v. Incline Vill. Gen. Imp. Dist.*, 597 F. Supp. 2d 1191, 1199 (D. Nev. 2009) (citing *Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 541 (1986)). Zappos argues that the TAC fails to establish Plaintiffs' standing to sue. This is considered a "facial" challenge to subject-matter jurisdiction. *Thornhill Publ'g Co. v. Gen. Tel. & Elec. Corp.*, 594 F.2d 730, 733 (9th Cir. 1979). "In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). If the movant's challenge is a facial one, then the "court must consider the allegations of the complaint to be true and construe them in the light most favorable to the plaintiff." *Nevada ex rel. Colo. River Comm'n of Nev. v. Pioneer Cos.*, 245 F. Supp. 2d 1120, 1124 (D. Nev. 2003) (citing *Love v. United States*, 915 F.2d 1242, 1245 (9th Cir. 1989)).

"Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010). When a party's allegations of injury rest on future harm, standing arises only if that harm is "*certainly* impending," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (internal quotation

marks and citation omitted), "or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2342 (2014) (citation omitted). Allegations "of *possible* future injury are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quotation marks and citation omitted). The alleged injury must be "'fairly traceable to the challenged action of the defendant,' rather than to 'the independent actions of some third party not before the court.'" *Ass'n of Pub. Agency Customers v. Bonneville Power Admin.*, 733 F.3d 939, 953 (9th Cir. 2013) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). A plaintiff does not need to show that a defendant's actions are the "proximate cause" of the plaintiff's injury, but a plaintiff "must establish a 'line of causation' between defendants' action and their alleged harm that is more than 'attenuated.'" *Maya v. Centex Corp.*, 658 F.3d 1060, 1070 (9th Cir. 2011) (quoting *Allen v. Wright*, 468 U.S. 737, 757 (1984)). The links of a causal chain must be plausible and not hypothetical or tenuous. *Id.* In addition, "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan*, 504 U.S. at 560-61 (quotations omitted).

The party invoking federal jurisdiction has the burden of establishing actual or imminent injury. *Id.* at 561. In a class action, the named plaintiffs attempting to represent the class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the

requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

III. DISCUSSION

A. Article III Standing

Zappos moves the Court to dismiss the TAC for lack of standing (ECF No. 254), whereas Prior Plaintiffs attempt to establish standing to revive their claims, and New Plaintiffs attempt to establish standing for the first time.

1. Prior Plaintiffs

In a previous order, the Court rejected in detail Prior Plaintiffs' three primary arguments for standing. First, the Court rejected the argument that standing exists because the data breach devalued Prior Plaintiffs' PII. The Court explained:

> Even assuming that Plaintiffs' data has value on the black market, Plaintiffs do not allege any facts explaining how their personal information became less valuable as a result of the breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach.

(Order, 6, ECF No. 235).

Second, the Court held that an increased threat of identity theft and fraud stemming from Zappos's security breach is insufficient to constitute an injury-in-fact. It found that Prior Plaintiffs' alleged damages rely almost entirely on conjecture and that not one of Prior Plaintiffs "alleges to have detected any

irregularity whatsoever in regards to unauthorized purchases or other manifestations that their personal information has been misused." (*Id.* at 12). The Court added: "three-and-a-half years after Zappos's security breach Plaintiffs have not sought leave to amend their Complaints to include any facts relating to instances of actual identity theft or financial fraud." (*Id.* at 16).

Third, the Court found that incurring costs to mitigate a threat cannot serve as the basis for this action. Although the Court found that Prior Plaintiffs lacked standing, it granted leave to amend the complaints for a third time "to allege instances of actual identity theft or fraud." (Order, 20).

In the TAC, Prior Plaintiffs still allege no instances of actual identity theft or fraud. Plaintiffs Hasner and Nobles re-allege that their email accounts were "accessed by hackers and used to send unwanted advertisements to people in [their] address book[s]." (TAC ¶¶ 34, 40). The Court has already rejected these allegations as insufficient to establish standing.[1] The only attempt Prior Plaintiffs make to revive their claims is to re-package their allegations that the data breach resulted in a devaluation of their personal information. They allege that when "[f]aced with the choice of having [their] PII wrongfully released . . . and otherwise used without [their]

[1] The Court noted that "[b]esides the advertisements . . . no additional misuse of the accounts or actual damages is alleged. Moreover, Hasner and Noble also took quick remedial measures by changing the passwords on their AOL accounts." (Order, 16, n.3). The Court held that "[i]n this case . . . there are no allegations of actual financial harm or that Plaintiffs' personal information has been disseminated over the Internet." (*Id.* at 16).

authorization," they would choose to sell their PII to receive compensation for it. (*Id.* ¶ 16). This allegation still does not allege any actual, concrete injury—it is merely conjectural. Prior Plaintiffs do not allege facts to show the value of their PII decreased following the data breach. For instance, they do not allege that their PII has been disseminated over the Internet or that any actual damage has occurred because of the breach. As the Court stated in its prior order, they do not allege "that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach." (Order, 6). Thus, even if Prior Plaintiffs' PII has actual market value, they have failed to allege any facts showing the data breach actually deprived them of any value attributable to this "unique and valuable property right." (TAC ¶ 15).

Once again, Prior Plaintiffs have failed to establish standing. As a result, the Court dismisses them from the case, this time with prejudice. Although "[t]he court should freely give leave [to amend] when justice so requires," Fed. R. Civ. Pro. 15(2), Prior Plaintiffs have failed to allege instances of actual identity theft or fraud, as the Court gave them leave to do. The Court dismisses Prior Plaintiffs' claims with prejudice.

2. New Plaintiffs

New Plaintiffs—O'Brien and Wadsworth—make the same general allegations as Prior Plaintiffs but also attempt to allege instances of actual identity theft and fraud. Zappos argues that New Plaintiffs have failed to allege any actual injury and that the injury is

not fairly traceable to the Zappos data breach. O'Brien makes three specific allegations:

> [O]n January 25, 2012, O'Brien . . . received a 'welcome letter' from Sprint thanking her for opening an account with two telephone lines and purchasing multiple telephones—none of which she did. The next day, she received a similar letter from AT&T regarding the purchase of three telephones she did not purchase. O'Brien spent a considerable amount of time (approximately two hours a day for a week and a half) on the telephone with Sprint and AT&T closing these accounts and extinguishing the account balances, including multiple telephone calls with an attorney to whom Sprint and AT&T had turned over the accounts for collection.
>
> Fraudsters also opened a Radio Shack in-store credit account in her name to which they charged over $400 of merchandise.
>
> Additional fraudulent purchases were made at Radio Shack using O'Brien's compromised Chase Visa credit card tied to her Zappos.com account.

(TAC ¶ 43). Wadsworth makes two allegations:

> [T]he fraudsters used her debit card to overdraw her bank account, which the bank unilaterally closed.
>
> The fraudsters also hacked her Paypal account, generating a $1000 balance that Paypal requires Wadsworth to pay in order to continue selling on Ebay. Until the balance is

> paid, her selling business, and corresponding revenue stream, are shut down.

(*Id.* ¶ 48).

These allegations are sufficient to establish standing. O'Brien and Wadsworth allege several types of injury they have suffered, including use of their credit, harm to their credit, lost time spent closing fraudulent accounts, and lost funds and business due to fraudulent charges. Zappos argues that the allegations of injury are merely conclusory and self-contradictory. For example, Wadsworth alleges that "[s]he utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis," (*id.* ¶ 47), but then she alleges that she "used the same . . . password on her Zappos.com and Ebay accounts," (*id.* ¶ 48). Although this apparent contradiction makes Wadsworth's allegations somewhat confusing, it is inconsequential because it appears that her first allegation is a general statement of her conduct, whereas the second involves the specific circumstances related to her allegations of fraud. Moreover, Wadsworth does not allege that fraudsters hacked her eBay account, just her Paypal account.

Zappos also argues that Wadsworth failed to allege "when her PayPal account was hacked or whether she used the same password on her Zappos and PayPal accounts." (Mot., 13, ECF No. 254). This lack of specificity is also inconsequential because "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that

are necessary to support the claim." *Lujan*, 504 U.S. at 561 (quotation omitted). Of course, at the summary judgment stage, "the plaintiff can no longer rest on such 'mere allegations,' but must 'set forth' by affidavit or other evidence 'specific facts.'" *Id.* (citation omitted).

The alleged injury is fairly traceable to the Zappos data breach. New Plaintiffs allege that hackers breached servers storing the PII of Zappos customers and stole the data, which Zappos admitted in an e-mail sent to its customers. They allege that following the data breach fraudulent activity occurred as a direct result of the breach. This chain of events is certainly plausible. They also allege that they "meticulously protect [their] PII" and have "never been victimized by a data breach other than the Zappos Data Breach." (TAC ¶¶ 42, 47).

Zappos argues that the alleged fraudulent activity is not fairly traceable to the Zappos data breach because "Plaintiffs do not allege any widespread fraudulent activity affecting Zappos's 24 million customers in the days or weeks (or now years) following the incident. . . . Given the lack of any allegations of widespread payment card fraud shortly following the incident, it is entirely implausible to conclude that complete credit/debit card data was stolen." (Mot., 12). Zappos also argues that Social Security numbers are necessary to open new credit accounts, and that Plaintiffs do not allege that Social Security numbers were stolen. (*Id.* at 13).

As time passes from the Zappos data breach and few Zappos customers have made allegations of actual fraud, it is a fair argument that fraudulent activity is less likely to have arisen from the Zappos breach and

more likely to have arisen from another source.[2] However, even if true, this argument does not preclude the possibility that the alleged injury is fairly traceable to the Zappos breach. First, Plaintiffs 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." (TAC ¶ 77). Second, although only two Zappos customers in the case have alleged actual injury resulting from the breach, New Plaintiffs present a list of customer complaints and records alleging misconduct shortly following the breach. (*Id.* ¶ 67). The list is brief, but additional discovery could uncover other allegations of actual fraud. Third, even if another data breach might have exposed New Plaintiffs' PII, Zappos has the burden to show its actions were not the "but for" cause of the injury. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015) ("If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but for' cause of the plaintiff's injury.'" (quoting *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J. concurring))). Fourth, even if the hackers did not steal full debit or credit card numbers or Social Security numbers, Plaintiffs allege that fraudsters can link various sources of information on the Internet "to create a mosaic of information."

---

[2] Data theft is fairly common. *See, e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 34 (D.D.C. 2014) ("roughly 3.3% of Americans will experience identity theft of some form, regardless of the source").

(TAC ¶ 56). Thus, although the Zappos breach might not have been the original source of all the information required to commit fraud, it might have been the catalyst, or a necessary link in the chain, that made the fraud possible. Finally, Zappos argues that the injuries are not fairly traceable to the Zappos breach because New Plaintiffs fail to allege when the actual fraud occurred. New Plaintiffs include a specific date in only one of their allegations, (*see id.* ¶ 42), but they generally allege that the fraudulent activity occurred after the data breach, which is sufficient.

At this stage, it is sufficient for purposes of standing to allege that Zappos sent its customers an e-mail notifying them that their PII had been compromised in a breach of its servers and that actual fraud occurred as a direct result of the breach. Whether or not New Plaintiffs' allegations suffer from defects that prevent them from ultimately prevailing in the case, the allegations show the connection between the alleged injury and breach is more than just hypothetical or tenuous. The Court finds that New Plaintiffs have standing.

B. Claims

1. California Claims

The Court grants the motion to dismiss the California claims (III, IV, and V) because New Plaintiffs (hereinafter "Plaintiffs") are not residents of California. Plaintiffs can move the Court to reconsider if they believe the California claims should proceed.

2. Breach of the Covenant of Good Faith and Fair Dealing; Breach of the Settlement Agreement

Plaintiffs were not parties to the case when Prior Plaintiffs and Defendant were discussing possible settlement. As a result, the Court dismisses the claims because Plaintiffs have no standing to make them.

3. Negligence/Negligent Misrepresentation

Zappos moves the Court to dismiss this claim for failure to state a claim. In a prior order, the Court dismissed Plaintiffs' simple negligence claim as barred by the economic loss doctrine because Plaintiffs failed to allege personal injury or property damage. (Order, 6-7, ECF No. 144). Plaintiffs now argue that their simple negligence claim is not barred by the economic loss doctrine because Zappos's duty to safeguard and protect their PII is imposed by state law. *See Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 879 (9th Cir. 2007) (holding that the economic loss doctrine "does not bar recovery in tort where the defendant had a duty imposed by law rather than by contract and where the defendant's intentional breach of that duty caused purely monetary harm to the plaintiff"). In the TAC, however, Plaintiffs make no allegation of any statutory duty. Moreover, although Plaintiffs allege actual economic injury for purposes of standing, they still fail to allege any personal injury or property damage. The Court will not revive the simple negligence claim.

In the prior order, the Court treated the simple negligence claim as a negligent misrepresentation claim, which the economic loss doctrine does not bar.

(*Id.* at 7-8). Zappos does not challenge this claim as alleged in the TAC.

4. Breach of Contract

Zappos moves the Court to dismiss the breach of contract claim for failure to state a claim. In the Court's prior order, it dismissed this claim with the following explanation:

> The only allegations alleged to give rise to any contract are that customers agreed to pay money for goods and that statements on Zappos's website indicated that its servers were protected by a secure firewall and that customers' data was safe. The first type of contract for the sale of goods is not alleged to have been breached, and the unilateral statements of fact alleged as to the safety of customers' data do not create any contractual obligations.

(Order, 6, ECF No. 114). The TAC does not make any new allegations that cure the deficiencies in the claim. Plaintiffs allege additional facts[3] that also constitute unilateral statements and, thus, fail to show that any contractual obligation existed. Plaintiffs also make additional allegations to support their claim that a contract existed because Zappos obtained value from Plaintiffs by possessing their PII, which they received in exchange for Zappos's promises to protect their PII.

---

[3] E.g., "Zappos also made a 'Safe Shopping Guarantee,' promising that the use of credit card information on its websites is secure. . . . Zappos also placed a yellow, lock-shaped icon on its website payment page that confirmed entry of a consumer's PII as part of an online retail transaction with Zappos was 'safe and secure.'" (TAC ¶¶ 59-60).

(*See* TAC ¶¶ 164-165). However, because the statements regarding PII safety are only unilateral, any value deriving from Plaintiffs' PII is only an incidental benefit of the contract for the sale of goods. Finally, Plaintiffs allege that they "relied on this covenant and, in fact, would not have disclosed their PII to Zappos without assurances that their PII would be properly safeguarded." (*Id.* ¶ 168). This allegation shows that Plaintiffs relied on Zappos's unilateral statements, but it does not show that Plaintiffs provided their PII to Zappos as consideration for Zappos's promise to protect it. Indeed, they allege that they "entrusted their confidential personal customer account information" to Zappos "[a]s part and parcel of their purchase transactions." (*Id.* ¶ 2). In other words, Plaintiffs provided their PII to Zappos as a means for completing an online transaction for the purchase of goods—not because Zappos was offering a service to protect Plaintiffs' PII. The Court dismisses the claim.

5. Unjust Enrichment

The elements of an unjust enrichment claim, or "quasi contract," include the following: "a benefit conferred on the defendant by the plaintiff, appreciation by the defendant of such benefit, and acceptance and retention by the defendant of such benefit under circumstances such that it would be inequitable for him to retain the benefit without payment of the value thereof." *Leasepartners Corp. v. Robert L. Brooks Trust*, 942 P.2d 182, 187 (Nev. 1997) (quotation omitted). A claim of unjust enrichment "is not available when there is an express, written contract, because no agreement can be implied when there is an express agreement." *Id.* (quotation

omitted). "The doctrine of unjust enrichment . . . applies to situations where there is no legal contract but where the person sought to be charged is in possession of money or property which in good conscience and justice he should not retain but should deliver to another or should pay for." *Id.* (quotation omitted).

In the Court's prior order, it dismissed Plaintiffs' unjust enrichment claim because they failed to allege that they conferred any benefit upon Zappos outside of the contracts they formed to purchase goods. (Order, 8-9, ECF No. 114). Plaintiffs have not cured this defect. They allege that it would be inequitable for Zappos to retain their PII without payment in light of the data breach; however, they also allege that they "entrusted their confidential personal customer account information" to Zappos "[a]s part and parcel of their purchase transactions." (TAC ¶ 2). Even if Zappos has benefitted from retaining Plaintiffs' PII, Zappos obtained it as part of the parties' contract for the sale of goods. Plaintiffs cannot maintain a claim of unjust enrichment based on that contract. Plaintiffs do not allege that they provided Zappos their PII for any other purpose that would make it inequitable for Zappos to retain the benefit of possessing their PII without payment. The Court dismisses the claim.

C. Motion to Strike

Zappos moves the Court to strike the class allegations from the TAC pursuant to Federal Rules of Civil Procedure 12(f)(2) and 23(d)(1)(D) (ECF No. 255). Plaintiffs argue that Zappos's motion is premature because class-related discovery has not been completed.

1. Legal Standards

Under Rule 12(f), "[t]he Court may strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." Rule 23(d)(1)(D) allows a court to "require that the pleadings be amended to eliminate allegations about representation of absent persons." Rule 23 does not prohibit a defendant from filing a motion to deny class certification before a plaintiff seeks to certify a class. *Vinole v. Countrywide Home Loans, Inc.*, 571 F.3d 935, 941 (9th Cir. 2009). Also, "[d]istrict courts have broad discretion to control the class certification process, and '[w]hether or not discovery will be permitted . . . lies within the sound discretion of the trial court.'" *Id.* at 942 (quoting *Kamm v. Cal. City Dev. Co.*, 509 F.2d 205, 209 (9th Cir. 1975)). In most cases, a district court should "'afford the litigants an opportunity to present evidence as to whether a class action was maintainable,'" *id.* (quoting *Doninger v. Pac. Nw. Bell, Inc.*, 564 F.2d 1304, 1313 (9th Cir.1977)), because "often the pleadings alone will not resolve the question of class certification and [thus] some discovery will be warranted," *id.* Class certification may be denied without discovery "where plaintiffs could not make a *prima facie* showing of Rule 23's prerequisites or that discovery measures were 'likely to produce persuasive information substantiating the class action allegations'"). *Id.* (citing and quoting *Doninger*, 564 F.2d at 1313).

To obtain class certification under Rule 23, Plaintiffs must show each of the following:

> (1) the class is so numerous that joinder of all members is impracticable;

> (2) there are questions of law or fact common to the class;
>
> (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and
>
> (4) the representative parties will fairly and adequately protect the interests of the class.

Rodriguez v. Hayes, 591 F.3d 1105, 1122 (9th Cir. 2010) (quoting Fed. R. Civ. P. 23(a)). Plaintiffs must also satisfy the requirements of Rule 23(b)(1)-(3). *Id.*

2. Analysis

The Court must strike the class allegations from the TAC. Plaintiffs propose the following nationwide class:

> All persons whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012. Excluded from the Nationwide Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

(TAC ¶ 90). Plaintiffs also propose a list of sub-classes of putative Plaintiffs in various states. (*Id.* ¶ 91), using language similar to the nationwide class. Although discovery is not complete and Plaintiffs have not yet moved to certify the class, the Court can strike the class allegations because it is clear from the face of the

TAC that Plaintiffs cannot make a prima facie showing of Rule 23's prerequisites.

In a prior order, the Court informed Plaintiffs that it "would not certify a class as broadly defined as Plaintiffs propose specifically because a majority of the putative class cannot claim any measurable damages." (Order, 19, ECF No. 235). Plaintiffs have failed to heed the Court's warning. The proposed class would include any person whose PII was compromised during the Zappos data breach, whether or not the person was the victim of actual fraud following the breach. The proposed class is far too broad, which prevents Plaintiffs from meeting the requirements of commonality and typicality.

The Court grants the motion to strike and gives Plaintiffs leave to amend to limit the proposed class to individuals who have suffered actual injury as a result of the Zappos data breach. If Plaintiffs attempt to narrow the proposed class, then the Court will entertain additional arguments for striking or certifying the class based on the revised class allegation.

D. Choice of Law

Zappos argues that Plaintiffs' claims must be limited to those pursued under Nevada law. Plaintiffs argue that claims under the laws of other states are appropriate. Given the Court's decision to grant Zappos's motion to strike the class allegations, the Court elects to defer to a later time a decision on the choice-of-law issue because whether Plaintiffs choose to amend their complaint to seek class certification will affect the Court's analysis. In addition, much of the parties' briefing on this issue focuses on the

circumstances involving Prior Plaintiffs rather than New Plaintiffs; thus, the Court would benefit from briefing that is more applicable and thorough in light of the changing circumstances of the case. The Court invites the parties to brief the issue fully when it is raised either in a motion to certify the class or another relevant motion.

E. Miscellaneous Motions

The parties have also filed several Motions to Seal (ECF Nos. 244, 248, 266) and a Motion for Leave to File Excess Pages (ECF No. 275). The Court grants the motions.

CONCLUSION

IT IS HEREBY ORDERED that Defendant's Motion to Dismiss (ECF No. 254) is GRANTED in part and DENIED in part, with leave to amend as indicated, within 30 days.

IT IS FURTHER ORDERED that Defendant's Motion to Strike (ECF No. 255) is GRANTED.

IT IS FURTHER ORDERED that the Motions to Seal (ECF Nos. 244, 248, 266) are GRANTED.

IT IS FURTHER ORDERED that Defendant's Motion for Leave to File Excess Pages (ECF No. 275) is GRANTED.

IT IS SO ORDERED.

Dated this 6th day of May, 2016

[handwritten: signature]
Robert C. Jones
United States District
Judge

Appendix F

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEVADA

No. 3:12-cv-00325
MDL No. 2357

IN RE ZAPPOS.COM, INC., CUSTOMER DATA SECURITY BREACH LITIGATION,

---

Filed: June 1, 2015

ORDER

This multidistrict litigation case arises out of a security breach of Zappos.com's customer data. Pending before the Court is a Motion to Dismiss, (ECF No. 217), filed by Amazon.com, Inc. doing business as Zappos.com ("Zappos"). Also pending is Zappos's Motion to Strike Prayers for Punitive Damages and Restitution. (ECF No. 219). Zappos has also filed a Motion for Leave to File Excess Pages. (ECF No. 218). The Court has considered all of the briefing on the pending Motions. For the reasons contained herein, the Motion to Dismiss is GRANTED, and the Motion to Strike is DENIED as moot.

I. FACTS AND PROCEDURAL HISTORY

On January 15, 2012, Zappos's servers located in Kentucky and Nevada were targeted by a hacker or group of hackers. The servers contained the personal identifying information of approximately 24 million

Zappos's customers. On January 16, 2012, Zappos sent an email to its customers notifying them that its servers had been breached and that data had been stolen, including customers' names, account numbers, passwords, email addresses, billing and shipping addresses, phone numbers, and the last four digits of their credit cards used to make purchases. Shortly thereafter, a number of lawsuits were filed against Zappos seeking damages.

On June 14, 2012, the U.S. Judicial Panel on Multidistrict Litigation ("JPML") granted Zappos's motion to create the present case pursuant to 28 U.S.C. § 1407, transferring six extra-district actions to this District, consolidating them with three actions from this District, and assigning the consolidated case to this Court. (Transfer Order, ECF No. 1). Zappos moved to compel arbitration and stay the case. While that motion was pending, the JPML transferred an additional action to be consolidated with the instant case. (Conditional Transfer Order, ECF No. 5). The Court denied the motion to compel arbitration because the arbitration contract was "browsewrap" not requiring any objective manifestation of assent (as opposed to a "clickwrap" agreement), and there was no evidence that Plaintiffs had knowledge of the offer such that assent could be implied merely by use of the website. (*See* Sept. 27, 2012 Order 7-10, ECF No. 21).

Plaintiffs then amended their pleadings into two separate consolidated class action complaints, and Zappos filed a motion to dismiss the amended complaints for lack of standing and for failure to state a claim. (ECF No. 62). On September 9, 2013, the Court granted in part and denied in part Zappos's

motion. (ECF No. 114). Thereafter, Plaintiffs Preira, Ree, Simon, Hasner, Habashy, and Nobles ("the Preira Plaintiffs") filed their Second Amended Consolidated Complaint (the "Preira SAC"). (ECF No. 118). And Plaintiffs Stevens, Penson, Elliot, Brown, Seal, Relethford, and Braxton (the "Stevens Plaintiffs") filed their Second Amended Consolidated Class Action Complaint (the "Stevens SAC"). (ECF No. 119).

On November 4, 2013, Zappos moved for dismissal of the Preira SAC and the Stevens SAC. (ECF No. 122). Zappos also moved to strike Plaintiffs' prayers for punitive damages and restitution. (ECF No. 124). While those motions were pending, the parties engaged in mediation in an attempt to reach a settlement. The parties stipulated to stay the proceedings various times, each time representing to the Court that settlement negotiations were progressing. (*See* ECF Nos. 192, 196, 201). After the third stipulation to stay, which was filed on September 17, 2014, and in reliance on the parties' representation that a settlement agreement was close, the Court entered an order denying Zappos's still pending motion to dismiss and motion to strike without prejudice. (ECF No. 202).

Despite the progress made during mediation as to class-wide relief, a final agreement could not be reached between the parties due to a disagreement over attorneys' fees. However, Plaintiffs filed a motion on December 4, 2014 to enforce a supposed settlement. (ECF No. 207), claiming that a cap on the fees class counsel would request was not material to the settlement. After responding to Plaintiffs' arguments regarding whether an enforceable settlement had

been reached, Zappos renewed its previous dismissal arguments by filing the instant Motions on January 30, 2015. (ECF Nos. 217, 219). Plaintiffs then requested an extension of time to oppose the Motions pending the Court's determination of the motion to enforce. On March 27, 2015, the Court, finding that no final settlement had been reached, denied the motion to enforce and ordered Plaintiffs to respond to the instant Motions so that the case might proceed. Accordingly, the Court now considers the merits of Zappos's Motion to Dismiss the Preira and Stevens SACs pursuant to Rule 12(b)(1) for lack of standing.

II. LEGAL STANDARD

"Lack of standing is a defect in subject-matter jurisdiction and may properly be challenged under Rule 12(b)(1)." *Wright v. Incline Vill. Gen. Imp. Dist.*, 597 F. Supp. 2d 1191, 1199 (D. Nev. 2009) (citing *Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 541 (1986)). Zappos argues that the Preira and Stevens SACs fail to establish Plaintiffs' standing to sue. This is considered a "facial" challenge to subject-matter jurisdiction. *Thornhill Publ'g Co. v. Gen. Tel. & Elec. Corp.*, 594 F.2d 730, 733 (9th Cir. 1979). "In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). If the movant's challenge is a facial one, then the "court must consider the allegations of the complaint to be true and construe them in the light most favorable to the plaintiff." *Nevada ex rel. Colo. River Comm'n of Nev. v. Pioneer Cos.*, 245 F. Supp. 2d

1120, 1124 (D. Nev. 2003) (citing *Love v. United States*, 915 F.2d 1242, 1245 (9th Cir. 1989)).

III. DISCUSSION

Zappos contends that Plaintiffs lack standing in this case because they have not alleged any actual damages arising from the data breach. Plaintiffs contend that their injury stems from an increased risk that they will become victims of identity theft or other fraudulent activities because their personal information has been jeopardized. None of the Plaintiffs, however, allege that they have suffered such harm as of yet. Moreover, only three of the twelve named Plaintiffs have taken the additional step of purchasing credit monitoring services to protect against the allegedly increased threat of fraud. In addition to the increased threat of harm, Plaintiffs further argue that they have standing based on damage to the intrinsic value of their data.

The Court was presented with similar arguments when ruling on Zappos's previous motion to dismiss. At that time, the Court determined that Plaintiffs' allegations "that they have had to pay money to monitor their credit scores and secure their financial information due to the increased risk of criminal fraud" were sufficient to establish standing. (Sept. 9, 2013 Order 5). However, given developments in the caselaw dealing with standing of data-breach victims, and because Article III standing is an "indispensable part of a plaintiff's case" rather than a pleading requirement, the Court finds it appropriate to review its prior ruling. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

"Standing under Article III of the Constitution requires that an injury be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010). When a party's allegations of injury rest on future harm, standing arises only if that harm is "*certainly* impending," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (internal quotation marks and citation omitted), "or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2342 (2014) (citation omitted). Allegations "of *possible* future injury are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quotation marks and citation omitted).

The party invoking federal jurisdiction has the burden of establishing actual or imminent injury. *Defenders of Wildlife*, 504 U.S. at 561. In a class action, the named plaintiffs attempting to represent the class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

1. Decreased value in Plaintiffs' personal information

The Court deals first with Plaintiffs' last theory of standing. Plaintiffs attempt to establish standing by

arguing that the data breach resulted in a devaluation of their personal information. Plaintiffs allege that a "robust market" exists for the sale and purchase of consumer data such as the personal information that was stolen during the breach, the value of this data apparently being appraised at between $ 30.49 and $44.62. (Stevens SAC ¶¶ 51-52). Plaintiffs claim that the Zappos security breach deprived them of the "substantial value" of their personal information, which they are entitled to recover. (*Id.* ¶ 54).

The Court does not buy this argument. Even assuming that Plaintiffs' data has value on the black market, Plaintiffs do not allege any facts explaining how their personal information became less valuable as a result of the breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach. *See Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 660 (S.D. Ohio 2014) (rejecting a similar argument because the named plaintiffs failed to allege that the data security breach actually prevented them from selling their information at the price they claimed the data was worth); *see also In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litg.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) (same). Thus, the Court finds that these allegations do not establish standing.

2. Increased threat of future harm

Plaintiffs' purported standing rests largely on the theory that they suffer an increased threat of future identity theft and fraud as a result of Zappos's security breach. Courts are divided on what constitutes sufficient injury-in-fact to establish standing in the

context of a data security breach. The division arises, at least in part, from the Supreme Court's recent holding in *Clapper v. Amnesty International*.

In *Clapper*, the plaintiffs, a group of lawyers, challenged the constitutionality of a section of the Foreign Intelligence Surveillance Act ("FISA") that authorizes surveillance of individuals who are not United States persons and are believed to be located outside of the United States. 133 S. Ct. at 1142. The plaintiffs alleged that their work required them to engage in sensitive international communication with individuals that they suspected were targets of surveillance under FISA. *Id.* There was no evidence, however, that their communications had been targeted or that the Government would imminently target their communications. Nevertheless, the plaintiffs claimed that their injury arose from an increased risk that their communications could be monitored in the future.

The Court held that the alleged harm was entirely speculative and did not support standing since the future injury was not "certainly impending." *Id.* at 1148. The Court explained that the plaintiffs' arguments "rest[ed] on their highly speculative fear" that (1) the Government would decide to target non-U.S. persons with whom they communicate; (2) that in doing so, the Government would choose to invoke its authority under FISA rather than some other method of surveillance; (3) that the Article III judges who serve on the Foreign Intelligence Surveillance Court would conclude the surveillance comported with the Fourth Amendment; (4) that the Government would succeed in intercepting communications of plaintiffs'

contacts; and (5) plaintiffs would be parties to the particular communications intercepted by the Government. *Id.*

This "highly attenuated chain of possibilities," the Court concluded, did not satisfy "the requirement that injury must be certainly impending." *Id.* The Court was also not willing "to abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors," *id.* at 1150, and it rejected the Second Circuit's reasoning that standing could be based on "an objectively reasonable likelihood" that the plaintiffs' communications with their foreign contacts would be intercepted in the future, *id.* at 1147.

The majority of courts dealing with data-breach cases post-*Clapper* have held that absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing. *See, e.g.*, *Green v. eBay Inc.*, No. CIV.A.14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (finding no standing where plaintiff's data was accessed during a security breach because there were no allegations that the information had been used or any indication that its use was imminent); *Storm v. Paytime, Inc.*, ---F. Supp. 3d---, No. 14-cv-1138, 2015 WL 1119724, at *6 (M.D. Pa. Mar. 13, 2015) (finding no standing where plaintiffs did not allege that they actually suffered any form of identity theft as a result of the defendant's data breach); *Peters v. St. Joseph Servs. Corp.*, ---F. Supp. 3d---, No. 4:14-cv-2872, 2015 WL 589561, *4-*5 (S.D. Tex. Feb. 11, 2015) (finding no standing where plaintiff did not allege actual identity theft or fraud despite the

possibility "that fraudulent use of her personal information could go undetected for long periods of time"); *Galaria*, 998 F. Supp. 2d at 654 (finding no standing where plaintiffs alleged their personal information was stolen and disseminated but did not allege that their data had been misused); *In re SAIC*, 45 F. Supp. 3d at 26 (finding no standing where plaintiffs allegations of potential identity theft, which had not yet occurred, were "entirely dependent on the actions of an unknown third party"); *Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014) (finding no standing where plaintiffs did not allege that identity theft had occurred but only that it "*may* happen in coming years"); *Remijas v. Neiman Marcus Grp., LLC*, No. 14c1735, 2014 WL 4627893, at *3 (N.D. Ill. Sept. 16, 2014) (finding no standing where plaintiffs' alleged injury was not "concrete" because it was based on "potential future fraudulent charges"); *Burton v. MAPCO Exp., Inc.*, No. 5:13-cv-00919-MHH, 2014 WL 4686479, at *1 (N.D. Ala. Sept. 12, 2014) (finding no standing despite plaintiff's allegations of unauthorized charges on his debit card because plaintiff did not allege that he actually had to pay for the charges); *U.S. Hotel & Resort Mgmt., Inc. v. Onity, Inc.*, No. CIV.13-1499, 2014 WL 3748639, at *5 (D. Minn. July 30, 2014) (recognizing that "[i]n the 'lost data' context . . . a majority of the courts . . . hold that plaintiffs whose confidential data has been exposed, or possibly exposed by theft or a breach of an inadequate computer security system, but who have not yet had their identity stolen or their data otherwise actually abused, lack standing to sue the party who failed to protect their data"); *In re Barnes & Noble Pin Pad*

Litig., No. 12-cv-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) ("Merely alleging an increased risk of identity theft or fraud is insufficient to establish standing.").

Courts in the Ninth Circuit, however, have held the opposite.[1] *See In re Adobe Sys., Inc. Privacy Litig.*, ---F. Supp. 3d---, No. 13-cv-05226-LHK, 2014 WL 4379916, at *8 (N.D. Cal. Sept. 4, 2014) (finding standing where hacker "spent several weeks" in Adobe's servers collecting customers' information despite no allegations that the plaintiffs' data had been misused); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (finding standing where the plaintiffs "alleged a 'credible threat' of impending harm" based on a data breach). These cases were decided in light of the Ninth Circuit's holding in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

In *Krottner*, employees of Starbucks sued the company when a laptop containing unencrypted names, addresses, and social security numbers of approximately 97,000 employees was stolen. 628 F.3d at 1140. Although some of the plaintiffs enrolled in credit monitoring services, they did not allege that any theft or other fraud actually occurred. *Id.* at 1142.

---

[1] Some courts outside the Ninth Circuit have also found standing in data breach cases where the plaintiffs do not allege actual identity theft or fraud, but those cases are relatively few. *See Moyer v. Michaels Stores, Inc.*, No. 14C561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014) (concluding "that the elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing").

Starbucks challenged the employees' standing since their allegations of harm were based solely on an "increased risk of future identity theft." *Id.* The court found the allegations sufficient to confer standing, holding that "[i]f a plaintiff faces 'a credible threat of harm' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III." *Id.* at 1143.

While other courts have criticized this test for being too lax post-*Clapper*, *see Peters*, 2015 WL 589561, at *6-*7 (recognizing the pre-*Clapper* split among the Third, Seventh, and Ninth Circuits on the issue of standing but finding that *Clapper* "[a]rguably . . . resolved the circuit split" and claiming that the *Clapper* "holding compels the conclusion" that plaintiffs lack standing to the extent the claims "are premised on the heightened risk of future identity theft/fraud"); *Galaria*, 998 F. Supp. 2d at 656 (finding that the reasoning in *Clapper* "seems to preclude the Ninth Circuit's even lower 'not merely speculative' standard for injury-in-fact" articulated in *Krottner*); *In re SAIC*, 45 F. Supp. 3d at 28 (impliedly accusing *Krottner* of being "thinly reasoned" and stating that, post-*Clapper*, the "'credible threat of harm' standard is clearly not supportable"), the *Adobe* and *Sony* courts found that *Clapper* did not overrule *Krottner* and that, in fact, *Clapper* and *Krottner* are quite compatible.

In *Sony*, the court found that "although the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be 'certainly impending,' rather than 'real and immediate,' the Supreme Court's

decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.'" 996 F. Supp. 2d at 961.

Likewise, the *Adobe* court reasoned that "*Clapper* did not change the law governing Article III standing." 2014 WL 4379916, at *7. "*Clapper* merely held that the Second Circuit had strayed from [the] well-established standing principles by accepting a too-speculative theory of future injury." *Id.* The court recognized the unique context in which *Clapper* was decided—a constitutional challenge to a national defense law—and concluded that *Krottner* and *Clapper* are not "clearly irreconcilable." *Id.* at *8. The court determined that the "difference in wording [between the two tests] is not substantial and that "*Krottner*'s phrasing is closer to *Clapper*'s 'certainly impending' language than it is to the Second Circuit's 'objectively reasonable likelihood' standard that the Supreme Court reversed in *Clapper*." *Id.*

This Court agrees that *Clapper* does not necessarily overrule *Krottner*. The *Krottner* test is composed of two parts: (1) the plaintiff must face "a credible threat of harm," *and* (2) "that harm [must be] 'both real and immediate.'" 628 F.3d at 1143. Both parts of the test must be met before the future harm equates to an injury-in-fact. Thus, it is not enough that a plaintiff face a credible threat of harm if that harm is not real, i.e. concrete, and immediate, i.e. certainly impending. *Krottner*, therefore, may be interpreted to require the same immediacy of harm that the Supreme Court emphasized in *Clapper*.

Furthermore, the Supreme Court explained post-*Clapper* 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." *Driehaus*, 134 S. Ct. at 2341 (emphasis added). So to the extent that the *Krottner* test is not as rigid as the standard articulated in *Clapper*, surely it embodies *Driehaus*'s "substantial risk" language.[2] Accordingly, this Court finds itself bound by *Krottner*. *See In re Adobe*, 2014 WL 4379916, at *8.

However, just because *Krottner* is controlling does not consequently mean that its outcome dictates the Court's conclusion as to standing here, due to the unique posture of this case. Immediacy is a common theme found in cases that discuss standing based on an alleged future harm. *See Nelsen v. King Cnty.*, 895 F.2d 1248, 1254 (9th Cir. 1990) (denying standing where plaintiffs failed to show "a credible threat of immediate future harm"). It is not enough that a credible threat may occur at some point in the future; rather, the threat must be impending. *See Defenders of Wildlife*, 504 U.S. at 564 (holding that a general

---

[2] *Clapper* recognized that future harm could create standing if the harm posed a "substantial risk." 133 S. Ct. at 1150 n.5; *see also Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153-54 (2010) (using this test to determine standing). In acknowledging this alternative articulation, though presumably not an alternative test, the Court stated that the impending harm does not need to be "literally certain." *Clapper*, 133 S. Ct. at 1150 n.5. Instead, the Court emphasized that "plaintiffs bear the burden of pleading and proving concrete facts showing that the defendant's actual action has caused the substantial risk of harm" and that plaintiffs "cannot rely on speculation about 'the unfettered choices made by independent actors not before the court.'" *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 562 (1992)).

intent to observe an endangered species in the future did not satisfy the immediacy requirement). It therefore follows that even if a plaintiff faces a real threat, she has no standing until that threat is immediate. *See Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (stating that "[a]llegations of possible future injury do not satisfy the requirements of Article III").

Similarly, a risk is surely not substantial unless the plaintiff can allege that the feared harm will likely be avoided only with judicial intervention. *See Monsanto Co.*, 561 U.S. at 152 (finding that plaintiffs would have been subjected to a substantial risk of future harm were it not for the district court's "elimination of [the] likelihood"). But where a credible threat will come to pass only if an independent third party takes specific action that would culminate in harm to the plaintiff, the alleged injury is less likely to confer standing. *See Clapper*, 133 S. Ct. at 1150.

Enter the facts of this case. Zappos's servers were breached in January 2012. Plaintiffs allege that the personal information of 24 million Zappos's customers was stolen. Of those 24 million customers, only twelve are before the Court seeking damages against Zappos. Of those twelve, only three determined that the increased threat of identity theft and fraud was sufficiently severe to purchase credit monitoring services. Of those three, not one alleges to have detected any irregularity whatsoever in regards to unauthorized purchases or other manifestations that their personal information has been misused. Yet Plaintiffs still claim that the threat they face is

immediate, though there is no indication when or if that threat will materialize.

Given the stipulated stays and other delays in this case, the Court must decide whether the alleged threat of future harm is properly considered certainly impending three-and-a-half years after the breach occurred. Even if Plaintiffs' risk of identity theft and fraud was substantial and immediate in 2012, the passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something. Determining what the lapsed time means, however, requires the Court to engage in speculation—precisely what the Supreme Court has counseled against. *Clapper*, 133 S. Ct. at 1149-50 (refusing standing based on speculation). It could signify that Plaintiffs are in the clear, meaning that the data obtained by the hacker was not useful in effectuating acts of theft or fraud. Or it could mean that the hacker is simply sitting on the information until the time is "right," which could be a few more years down the road. Or the lapsed time might mean a number of other scenarios. It is simply unclear.

If the Court assumes that the hacker or some other nefarious third-party remains in possession of Plaintiffs' personal information, then the threat may as yet be credible. In fact, Plaintiffs claim that cybercriminals "often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves," (Preira SAC ¶ 21; Stevens SAC ¶ 42), indicating that the alleged harm is not merely speculative despite the years that have passed without an occurrence of theft or fraud. But a harm

that is "not merely speculative" does not constitute an injury-in-fact sufficient to confer standing. *See Galaria*, 998 F. Supp. 2d at 656.

Indeed, there must be a point at which a future threat can no longer be considered certainly impending or immediate, despite its still being credible; otherwise, an "objectively reasonable likelihood" of harm would be enough to establish standing. *See id.* (citing *Clapper*, 133 S. Ct. at 1147). After all, the plaintiffs in *Clapper* engaged in the exact type of communication that could be monitored under FISA, making their allegations of future harm quite credible even if not certainly impending. *Clapper*, 133 S. Ct. at 1148-50. The more time that passes without the alleged future harm actually occurring undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial. *See Storm*, 2015 WL 1119724, at *6 ("Indeed, putting aside the legal standard for imminence, a layperson with a common sense notion of 'imminent' would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future.").

The Court therefore finds that the increased threat of identity theft and fraud stemming from the Zappos's security breach does not constitute an injury-in-fact sufficient to confer standing. The years that have passed without Plaintiffs making a single allegation of theft or fraud demonstrate that the risk is not immediate. *Krottner*, 628 F.3d at 1143. The possibility that the alleged harm could transpire in the as-of-yet undetermined future relegates Plaintiffs' injuries to the realm of speculation. *See Green*, 2015

WL 2066531, at *4 (finding the threat of identity theft and fraud not certainly impending because, rather than alleging actual theft or fraud, plaintiff claimed that he had to "be vigilant *for many years* in checking for fraud" because criminals "may hold the information for later use").

The degree of Plaintiffs' speculation is heightened further by the fact that the future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor. *Clapper*, 133 S. Ct. at 1150 (refusing to endorse standing that rests on speculation about the decisions of independent actors). Should the person or persons in possession of Plaintiffs' information choose not to misuse the data, then the harm Plaintiffs fear will never occur. Likewise, if the person or persons in possession of Plaintiffs' information are unable to use the data to wreak the havoc assumedly intended, then Plaintiffs' alleged damages would also not coalesce. *See Peters*, 2015 WL 589561, at *5 (acknowledging that the risk of future harm to the victim of a data security breach is, "no doubt, indefinite," but finding that the plaintiff's allegations of future harm were based solely on conjecture). Plaintiffs' damages at this point rely almost entirely on conjecture. *See Krottner*, 628 F.3d at 1143 (holding that standing cannot be based on conjecture but must be real and immediate).

The Court also notes the factual differences between the instant case and the *Adobe* and *Sony* cases. In *Adobe*, the plaintiffs alleged that the hackers had spent several weeks targeting Adobe's systems and that the hackers used Adobe's own system to decrypt customer credit cards. 2014 WL 4379916, at

*8. Not only were entire credit card numbers obtained, but some of the stolen data began to surface on the Internet within a year of the breach. *Id.* The hackers had even utilized the information to discover vulnerabilities in Adobe's products. *Id.* It was therefore clear that the threat faced by the *Adobe* plaintiffs was certainly impending. In *Sony*, the named plaintiffs were deprived of services as a result of the security breach for which they had paid money, and at least some of the plaintiffs had experienced unauthorized charges to their credit cards and one plaintiff was forced to close two bank accounts. 996 F. Supp. 2d at 956-57.

Unlike the plaintiffs in *Adobe* whose entire credit card numbers were stolen as a result of the security breach, Plaintiffs here allege that only their credit card "tails," the last four digits of a credit card, were accessed during Zappos's breach. Also unlike the plaintiffs in *Adobe* whose information began to surface on the Internet shortly after the breach, Plaintiffs here make no allegations that their data has appeared in any place where others might obtain and misuse it. Unlike the plaintiffs in *Sony* who experienced an actual loss, albeit temporarily, of the services for which they had paid Sony to provide, the usefulness of the goods Plaintiffs purchased from Zappos was in no way impacted by the security breach in this case. And unlike some of the plaintiffs in *Sony* who dealt with actual unauthorized charges on credit cards, Plaintiffs here do not allege one instance of financial fraud.

But perhaps the most distinguishing element between this case and *Adobe* and *Sony* is the amount of time from when the breach occurred to when the

respective motions to dismiss were ruled upon. In *Adobe*, the data security breach occurred in July and August of 2013. 2014 WL 4379916, at *2. The cases against Adobe were filed between November 2013 and January 2014. *Id.* The Court ruled on the motion to dismiss on September 4, 2014, just over a year from when the breach first occurred. So recently after the breach, and given that the plaintiffs' information had already begun showing up on the Internet, the court reached the reasonable conclusion that the threat of additional harm was imminent. Similarly, the court in *Sony* ruled on the issue of Article III standing on January 21, 2014, approximately two-and-a-half years after the breach in that case had occurred. 996 F. Supp. 2d at 955. Given the actual financial damages allegedly experienced by the named plaintiffs, the threat of future additional harm remained imminent at that time. In this case, however, there are no allegations of actual financial harm or that Plaintiffs' personal information has been disseminated over the Internet.[3] Instead, three-and-a-half years after Zappos's security breach Plaintiffs have not sought leave to amend their Complaints to include any facts relating to instances of actual identity theft or financial fraud.

---

[3] Plaintiffs Hasner and Noble do allege that after the breach, their AOL email accounts were accessed by a third party who sent unauthorized advertisements to others from the accounts. (Preira SAC ¶¶ 11, 16). The AOL accounts used the same passwords as Hasner's and Noble's Zappos accounts. Besides the advertisements, however, no additional misuse of the accounts or actual damages is alleged. Moreover, Hasner and Noble also took quick remedial measures by changing the passwords on their AOL accounts. (*Id.*).

Finally, even if Plaintiffs suffer identity theft or fraud at some point in the future, there may be a genuine issue regarding whether the Zappos's security breach is the reason for the damages then incurred. *Peters*, 2015 WL 589561, at *5 ("It may even be impossible to determine whether the misused information was obtained from exposure caused by the Data Breach or from some other source."). While this is obviously a question for another day, the Court notes that Plaintiffs would of course have to show that any damage occurring in the future is fairly traceable to the Zappos's breach. *Monsanto Co.*, 561 U.S. at 149. Since today so much of our personal information is stored on servers just like the ones that were hacked in this case, it is not unrealistic to wonder whether Plaintiffs' hypothetical future harm could be traced to Zappos's breach. An inference could of course be drawn that the future harm arose from Zappos's breach, but it would be Plaintiffs' burden to establish that element of standing. *Defenders of Wildlife*, 504 U.S. at 561. For all these reasons, the Court finds that Plaintiffs have not alleged a threat of future harm sufficiently imminent to confer standing under *Clapper* and *Krottner*.

2. Costs to mitigate

Plaintiffs Hasner, Preira, and Habashy next argue that even if the increased threat of future harm does not constitute an injury-in-fact, their purchasing of credit monitoring services does. However, in *Clapper* the Supreme Court rejected a similar argument raised by the plaintiffs there that they had standing because of expenditures made to protect the confidentiality of their communications. 133 S. Ct. at

1151. The Court explained that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.*

Courts have generally interpreted this holding to mean that "in order for costs incurred in an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm being mitigated must itself be imminent." *In re Adobe*, 2014 WL 4379916, at *9; *see also Storm*, 2015 WL 1119724, at *7 (finding no compensable injury when plaintiff incurred credit monitoring costs); *In re SAIC*, 45 F. Supp. 3d at 26 ("The cost of credit monitoring and other preventative measures, therefore, cannot create standing."). The Court's finding here that the threat of future theft or fraud is not sufficiently imminent to confer standing compels the conclusion that incurring costs to mitigate that threat cannot serve as the basis for this action. *See Clapper*, 133 S. Ct. at 1151 ("Thus, allowing respondents to bring this action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of respondents' first failed theory of standing.").

The Court realizes that this is a frustrating result where Plaintiffs' fears of identity theft and fraud are rational, and it recognizes that purchasing monitoring services is a responsible response to a data breach. Nevertheless, costs incurred to prevent future harm is not enough to confer standing, *Clapper*, 133 S. Ct. at

1150-51, "even when such efforts are sensible," *In re SAIC*, 45 F. Supp. 3d at 26. "There is, after all, nothing unreasonable about monitoring your credit after a data breach," but even when fears of future harm are not unfounded, plaintiffs simply "cannot create standing by 'inflicting harm on themselves' to ward off an otherwise speculative injury." *Id.* (quoting *Clapper*, 133 S. Ct. at 1151).[4]

As one court reasoned:

> Hackers are constantly seeking to gain access to the data banks of companies around the world. Sometimes, they are successful. Other times not. Despite many companies' best efforts and tremendous expense to secure and protect their data systems, an industrious hacker every so often may find a way to access their data. Millions of people, out of reasonable fear and prudence, may decide to incur credit monitoring costs and take other preventative steps, which the hacked companies often freely provide. However, for a court to require companies to pay damages to thousands [and in this case millions] of

[4] The Court finds this to be true notwithstanding Zappos's questionable customer service in response to the data breach. Plaintiffs allege that once Zappos notified customers of the breach it "shut down its customer service phone lines for a week." (Preira SAC ¶ 4). Also perplexing, and undoubtedly offensive to its customers, is Zappos's apparent decision to not offer free credit monitoring services to its customers, which is a common gesture in these types of cases. Nevertheless, these deficiencies in Zappos's customer care do not establish standing where Plaintiffs fail to allege actual damages or an immediate threat of future harm.

> customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to business. There is simply no compensable injury yet, and courts cannot be in the business of prognosticating whether a particular hacker was sophisticated or malicious enough to both be able to successfully read and manipulate the data and engage in identity theft.

Storm, 2015 WL 1119724, at *7. However, once a third party misuses a person's personal information, there is clearly an injury that can be compensated with money damages. *Id.* "In that situation, a plaintiff would be free to return to court and would have standing to recover her losses." *Id.*

To the extent that Plaintiffs allege that there are potential class members who have suffered identity theft or other fraud as a result of the Zappos's security breach, (*see* Preira SAC ¶¶ 5, 35), the Court agrees that those individuals would have standing. Yet Plaintiffs would not be the proper representatives of such a class, as they do not allege that they have suffered these same damages. *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 156 (1982) ("We have repeatedly held that a class representative must be part of the class and possess the same interest and suffer the same injury as the class members."). Moreover, even if this case were not dismissed for lack of standing, the Court would not certify a class as broadly defined as Plaintiffs propose specifically because a majority of the putative class cannot claim any measurable damages.

Therefore, based on the forgoing reasons, the Court is granting Zappos's Motion to Dismiss.[5] But the Court is also granting Plaintiffs leave to amend their Complaints for a third time in the event an occurrence of actual misuse of the stolen data has transpired between the dates the Preira and Stevens SACs were filed and now. And although the Court finds no standing based on the facts as currently pleaded, the case will be dismissed without prejudice.

---

[5] Plaintiffs claim they have standing on the alternative theories that the breach caused them a loss of privacy and that it resulted in a diminished value of the services provided by Zappos. (Resp. 5, ECF No. 231). Neither of these arguments is persuasive. Even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury. *See O'Shea v. Littleton*, 414 U.S. 488, 493 (1974) ("Abstract injury is not enough. It must be alleged that the plaintiff 'has sustained or is immediately in danger of sustaining some direct injury' as a result of [the defendant's] conduct."). Plaintiffs do not claim that they have suffered any damages due to a loss of privacy, and so the Court finds that this theory is insufficient to establish standing. Furthermore, Plaintiffs' claims that they are harmed by an alleged decrease in the value of Zappos's services are unavailing. Plaintiffs do not explain how the data breach impacted the value of the goods they purchased from Zappos. Nor do Plaintiffs allege facts showing how the price they paid for such goods incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data. The Court finds that this theory of standing also fails. To the extent Plaintiffs claim to have standing arising from any other perceived harm, (*see* Resp. 5), the Court finds that each proposed theory fails because not one of them demonstrates that Plaintiffs have actually been damaged in a concrete and particularized way. *See O'Shea*, 414 U.S. at 493.

CONCLUSION

IT IS HEREBY ORDERED that Defendant's Motion to Dismiss (ECF No. 217) is GRANTED without prejudice. Plaintiffs are granted leave to amend their Complaints to allege instances of actual identity theft or fraud.

IT IS FURTHER ORDERED that Defendant's Motion to Strike (ECF No. 219) is DENIED as moot.

IT IS FURTHER ORDERED that Defendant's Motion for Leave (ECF No. 218) is GRANTED.

IT IS SO ORDERED.

Dated: June 1, 2015

[handwritten: signature]
Robert C. Jones
United States District
Judge

Appendix G

U.S. Const. art. III, §§ 1-2

Section 1.

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

Section 2.

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public Ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

In all Cases affecting Ambassadors, other public Ministers and Consuls, and those in which a State shall be Party, the supreme Court shall have original Jurisdiction. In all the other Cases before mentioned, the supreme Court shall have appellate Jurisdiction,

both as to Law and Fact, with such Exceptions, and under such Regulations as the Congress shall make.

The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed.