No. 16-16860

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THERESA STEVENS, DAHLIA HABASHY, PATTI HASNER, SHARI SIMON, STEPHANIE PRIERA, KATHRYN VORHOFF, DENISE RELETHFORD and ROBERT REE,

Plaintiffs-Appellants,

v.

ZAPPOS.COM, INC.,

Defendant-Appellee.

Panel Opinion Filed: March 8, 2018

DEFENDANT-APPELLEE'S PETITION FOR PANEL REHEARING OR ALTERNATIVELY FOR REHEARING *EN BANC*

Julia B. Strickland
Stephen J. Newman
Brian C. Frontino
David W. Moon
STROOCK & STROOCK & LAVAN LLP
2029 Century Park East
Los Angeles, California 90067
310-556-5800

Robert McCoy
KAEMPFER CROWELL
1980 Festival Plaza Drive, Suite 650
Las Vegas, Nevada 89101
702-792-7000

Counsel for Defendant-Appellee ZAPPOS.COM, INC.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, defendant-appellee Zappos.com, Inc. ("Zappos") discloses that its parent corporation, Amazon.com, Inc., a publicly held corporation, owns 100% of Zappos.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

RULE 35(B) STATEMENT

In counsel's judgment, the panel's opinion (attached as Exhibit 1) satisfies one or more of the situations described in the "purpose" section of the Court's Information Regarding Judgment and Post-Judgment Proceedings (Dkt. 61-2). As set forth in greater detail below, the Court should grant panel rehearing because "[a] material point of fact or law was overlooked in the decision" and "[a]n apparent conflict with another decision of the Court was not addressed in the opinion." (Dkt. 61-2.)[1] Alternatively, the Court should grant rehearing *en banc* because "[c]onsideration by the full Court is necessary to secure or maintain uniformity of the Court's decisions" and "[t]he opinion directly conflicts with an existing opinion by another court of appeals or the Supreme Court and substantially affects a rule of national application in which there is an overriding need for national uniformity." (Id.)[2]

[1] See Town of Chester, N.Y. v. Laroe Estates, Inc., 137 S. Ct. 1645, 1650-51 (2017); Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016); Rockwell Int'l Corp. v. United States, 549 U.S. 457, 473-74 (2007); Northstar Fin. Advisors Inc. v. Schwab Invs., 779 F.3d 1036, 1044-45 (9th Cir. 2015).

[2] See id.; Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013); In re SuperValu, Inc., 870 F.3d 763, 770-27 (8th Cir. 2017); Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

I. INTRODUCTION

This appeal addresses whether consumers who do not allege that they suffered any identity theft or fraud as a result of an alleged data security breach can meet the injury in fact requirement for Article III standing. The alleged breach occurred more than three and a half years before the filing of the operative amended complaint, and the appellants here, the "Prior Plaintiffs,"[3] argue for standing on the grounds that they may become victims of identity theft or fraud in the future. The district court rejected this argument, holding that Prior Plaintiffs lacked standing because their alleged future injury was not "certainly impending" given the significant lapse of time and lack of alleged personal harm. The panel reversed, finding that it must assess the likelihood of future injury as of the filing of the initial complaint and that the passage of three and a half years without any harm could not even be considered in evaluating the likelihood of future injury. The Court should now grant panel rehearing or rehearing *en banc*.

First, the panel found that it must assess standing as of January 16, 2012, when the first plaintiff filed the first class action complaint. But the panel should have assessed standing as of September 28, 2015, when plaintiffs filed the operative Third Amended Consolidated Complaint ("Operative Complaint"). The

[3] "Prior Plaintiffs" are Theresa Stevens, Dahlia Habashy, Patti Hasner, Shari Simon, Stephanie Priera, Kathryn Vorhoff, Denise Relethford and Robert Ree. "New Plaintiffs" are Kristin O'Brien and Terri Wadsworth. Prior Plaintiffs are parties to this appeal; New Plaintiffs are not. (See Op. 14.)

panel's finding was error because it directly conflicts with Rockwell International Corp. v. United States, 549 U.S. 457, 473-74 (2007), and Northstar Financial Advisors Inc. v. Schwab Investments, 779 F.3d 1036, 1044-45 (9th Cir. 2015). Rockwell and Northstar instruct courts to assess standing based on the facts existing at the time the operative complaint is filed, not (as the panel held) at the time the original complaint is filed. This distinction is critical here. Given the unusual procedural history of this case, more than three and a half years elapsed between the incident at issue (as well as the filing of the initial complaint) and the filing of the Operative Complaint. Courts across the country have approvingly cited the district court's finding that a substantial lapse in time following a data breach undermines a determination that future harm is imminent. The Court should grant panel rehearing or rehearing *en banc* to resolve the conflict with Rockwell and Northstar (and with the other courts that have relied on the analysis of the district court below), and the Court should rule that standing should be assessed as of the filing of the Operative Complaint.

Second, even if standing is assessed based on the initial complaint, the Court should grant rehearing to correct an inconsistency in the panel's analysis. In holding that Prior Plaintiffs sufficiently alleged a substantial risk of identity theft or fraud, the panel credited allegations in the Operative Complaint made by the two New Plaintiffs (whose claims were voluntarily dismissed with prejudice)

regarding harm they allegedly suffered after the filing of the initial complaint. The panel's reliance on these allegations is inconsistent with its refusal to consider the passage of time between the initial complaint and the Operative Complaint. Either: (i) the initial complaint controls, and therefore the panel cannot consider allegations that appeared for the first time in the Operative Complaint; or (ii) the Operative Complaint controls, and the panel must consider (as the district court correctly considered) the significance of the passage of three and a half years without any actual harm suffered by Prior Plaintiffs.

Third, the panel's holding that Prior Plaintiffs sufficiently alleged standing based on a substantial risk of future identity theft or fraud, even though they did not allege any actual identity theft or fraud, directly conflicts with recent opinions by the Second, Fourth, and Eighth Circuits. This conflict merits rehearing *en banc*.

Fourth, rehearing *en banc* is necessary because, contrary to the panel's opinion, Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013), effectively overruled the authority upon which the panel relied, Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010). Clapper's "certainly impending" injury standard controls here because it is inconsistent with Krottner's "credible threat of harm" standard. Krottner fails to satisfy the case-or-controversy standard of Article III of the Constitution, as construed by the Supreme Court.

For all these reasons, the Court should grant panel rehearing or rehearing *en banc*.

II. BACKGROUND

On January 15, 2012, Zappos emailed notice to its customers that a computer hacker (or group of hackers) accessed Zappos's computer servers without authorization and may have accessed, among other things, certain customers' credit card "tails" (the last four digits of a credit card number). (ER 221, 248.) The initial complaint against Zappos was filed on January 16, 2012, similarly alleging that hackers stole only credit card tails, not full credit card numbers. (See Stevens v. Amazon.com, Inc., No. 12-cv-00032, ECF No. 1 at ¶1 (W.D. Ky. Jan. 16, 2012).)

On June 14, 2012, the United States Judicial Panel on Multidistrict Litigation transferred and coordinated nine actions in the District Court of Nevada. (ER 193.) On November 12, and 13, 2012, Prior Plaintiffs filed two sets of consolidated amended complaints. (ER 200.) On September 9, 2013, the district court granted in part and denied in part Zappos's motion to dismiss, finding that Prior Plaintiffs generally had standing. (ER 56-68.) On October 7, 2013, Prior Plaintiffs voluntarily filed two sets of consolidated second amended complaints. (ER 205.) Like all eleven complaints preceding them, the two second amended complaints did not allege that hackers obtained Prior Plaintiffs' complete credit

card data or that Prior Plaintiffs suffered any identity theft or fraud resulting from the Zappos incident. (ECF Nos. 118, 119.)

On June 1, 2015, the district court entered an order dismissing with leave to amend the second amended complaints for lack of standing. (ER 30-49.) In particular, the district court rejected Prior Plaintiffs' theory that they had standing due to an alleged increased risk of future identity theft and fraud, reasoning that the long time that had passed, without a single allegation of an actual or attempted theft or fraud against Prior Plaintiffs, demonstrated that Prior Plaintiffs' risk of future harm was not immediate and that their alleged damages "rely almost entirely on conjecture." (ER 43-44.)

On September 28, 2015, Prior Plaintiffs, joined for the first time by the two New Plaintiffs, filed the Operative Complaint. (ER 100-176.) For the first time, the Operative Complaint alleged that hackers accessed full debit and credit card information in the January 2012 incident. (ER 248.) Additionally, while Prior Plaintiffs again failed to allege any actual or attempted fraud or identity theft against them, New Plaintiffs did. (ER 225-244.) On May 6, 2016, the district court granted in part and denied in part Zappos's motion to dismiss. (ER 13-29.) The district court found that New Plaintiffs plausibly alleged standing but that Prior Plaintiffs once again did not. (ER 17-19.) Even though the district court permitted New Plaintiffs to proceed with litigation, New Plaintiffs chose to dismiss

their claims with prejudice, and the district court entered final judgment on September 13, 2016. (ER 218-219.)

III. REASONS TO GRANT THE PETITION

A. The Panel's Evaluation of Standing as of the Filing of the Initial Complaint Is Contrary to United States Supreme Court and Ninth Circuit Authority.

The panel held that the Court must "assess Plaintiffs' standing as of January 2012," when the first plaintiff filed a complaint, instead of September 28, 2015, when plaintiffs filed the Operative Complaint. (Op. 14.) The panel's decision—reached without the benefit of briefing from the parties on the issue—should be reconsidered because it directly conflicts with binding Supreme Court and Ninth Circuit precedent.

"[W]hen a plaintiff files a complaint in federal court and then voluntarily amends the complaint, courts look to the *amended complaint* to determine jurisdiction." Rockwell, 549 U.S. at 473-74 (emphasis added). This is because "[t]he state of things and the originally alleged state of things are not synonymous[.]" Id. at 473. Thus, "while later events may not create jurisdiction where none existed at the time of filing, the proper focus in determining jurisdiction are the *facts existing at the time the complaint under consideration was filed*." Northstar, 779 F.3d at 1044-45 (emphasis added). For example, in Northstar, plaintiff filed an action on behalf of mutual fund investors before

obtaining an assignment of claims from any fund investor, as required to establish standing. See id. at 1043. Approximately three months later, Northstar obtained an assignment of claims and subsequently filed an amended complaint. Id. The Ninth Circuit rejected defendant's argument that standing must be determined at the time an action is filed and that subsequent events (in that case, the assignment of claims) could not cure the original lack of standing. Id. Indeed, consistent with this principle, the Ninth Circuit regularly analyzes the allegations in *amended* complaints to assess standing. See, e.g., Carrico v. City & County of San Francisco, 656 F.3d 1002, 1006 (9th Cir. 2011); Barnum Timber Co. v. EPA, 633 F.3d 894, 895, 897 (9th Cir. 2011); see also In re SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017) (analyzing allegations in amended complaint to determine whether data breach plaintiffs had standing).

Here, the panel relied on Mollan v. Torrance, 22 U.S. 537, 539 (1824), which states that a party's citizenship for purposes of assessing diversity jurisdiction "depends upon the state of things at the time of the action brought." But Plaintiffs did not cite Mollan in their appellate briefs and did not argue that standing is assessed as of the initial complaint. Thus, Zappos did not have the opportunity to address Mollan before the panel issued its opinion.

The panel's reliance on Mollan is misplaced. In cases where jurisdiction depends on where a party is domiciled, "courts look to prevent defendants from

conspiring to deprive the court of jurisdiction by moving into the state following the filing of suit." Powder River Basin Res. Council v. Babbitt, 54 F.3d 1477, 1485 (10th Cir. 1995). In contrast, in standing cases, "if a plaintiff is no longer injured, courts lack a true 'case or controversy' upon which to render a decision." Id.[4] Thus, the district court in this case correctly considered the alleged facts (or lack thereof) in the Operative Complaint to evaluate standing. Indeed, in Northstar, the Ninth Circuit expressly rejected diversity jurisdiction cases as precedent when conducting a standing analysis with respect to an amended complaint. See Northstar, 779 F.3d at 1047 ("[T]he present case does not involve the issue of diversity jurisdiction.").

The difference between assessing standing as of the initial complaint and as of the Operative Complaint is dispositive. For example, on September 9, 2013, the district court initially found that Prior Plaintiffs had standing due to an alleged increased risk of future identity theft and fraud. (ER 56-68.) After years passed, however, the district court correctly rejected that theory of standing due to the

[4] Indeed, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997)). "Most standing cases consider whether a plaintiff has satisfied the requirement when filing suit, but Article III demands that an 'actual controversy' *persist throughout all stages of litigation*." Hollingsworth v. Perry, 570 U.S. 693, 705 (2013) (emphasis added) (citing Already, LLC v. Nike, Inc., 568 U.S.85, 90-91 (2013)).

significant passage in time and lack of alleged personal harm suffered by Prior Plaintiffs. (ER 43-44.)

Numerous courts across the country have cited the district court's analysis, approvingly, on this exact issue. See, e.g., Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) ("as the breaches fade further into the past, the Plaintiffs' threatened injuries become more and more speculative"); Duqum v. Scottrade, Inc., No. 15-cv-1537, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016) ("[A]s more time lapses without the threatened injury actually occurring, the notion that the harm is imminent becomes less likely."); Chambliss v. Carefirst, Inc, 189 F. Supp. 3d 564, 570 (D. Md. 2016) ("The imminence of the asserted harm thus becomes ever less likely as the breaches fade further into the past."). Because the panel's decision to assess standing as of the initial complaint directly conflicts with Rockwell, Northstar and other authorities, the Court should grant panel rehearing or rehearing *en banc*.[5]

[5] If the panel agrees with Zappos and considers all allegations (or lack thereof) in the Operative Complaint on rehearing, it also should address Zappos's argument that Prior Plaintiffs' credit card allegations in the Operative Complaint are not plausible. (See Appellee's Br. 19-20.) Although Prior Plaintiffs allege in the Operative Complaint—contrary to their prior allegations—that full debit and credit card information was accessed in the Zappos incident, Prior Plaintiffs do not allege that *their* debit or credit card accounts ever were improperly used. Given the lack of any allegations of widespread payment card fraud affecting Zappos's 24 million customers, or of any attempts at fraud specifically directed to Prior Plaintiffs, plaintiffs' contradictory credit card allegations should be rejected as implausible.

B. The Panel Improperly Considered Harm Allegedly Suffered by New Plaintiffs After the Filing of the Initial Complaint.

Regardless of whether standing is assessed as of the initial complaint (which it is not, under Northstar), panel rehearing is needed because the panel improperly found that Prior Plaintiffs have standing based on harm allegedly suffered by New Plaintiffs after the filing of the initial complaint. This is both logically inconsistent and prohibited by recent Supreme Court authority holding that one party may not rely on another party's injury to establish his own standing.

In finding that Prior Plaintiffs sufficiently alleged a substantial risk of identity theft or fraud, the panel relied on allegations that hackers "commandeered" New Plaintiffs' financial accounts or identities. (See Op. 13-14.) But that harm allegedly occurred *after* the filing of the initial complaint on January 16, 2012. (See, e.g., ER 240 (alleging that one New Plaintiff received a letter on January 25, 2012 about the opening of an unauthorized telephone account with Sprint).) Because the alleged harm had not yet occurred, those allegations were of course not in the initial complaint (or any of the thirteen complaints preceding the Operative Complaint). The panel therefore considered events that allegedly occurred after the filing of the initial complaint that supposedly support standing, but refused to consider events that did *not* occur after the filing of the initial complaint that undermine standing. The panel's selective consideration of events occurring after the filing of the initial complaint is logically inconsistent.

In addition, the panel's consideration of harm allegedly suffered by New Plaintiffs (who voluntarily dismissed their claims with prejudice) is barred by Supreme Court precedent. In Town of Chester, N.Y. v. Laroe Estates, Inc., 137 S. Ct. 1645, 1650-51 (2017), the Supreme Court applied the principle that "standing is not dispensed in gross" to find that a proposed intervenor did not have standing based on injuries sustained by the existing plaintiff to the litigation. "For all relief sought, there must be a litigant with standing, whether that litigant joins the lawsuit as a plaintiff, a coplaintiff, or an intervenor of right." Id. at 1651. Yet here, the panel found that Prior Plaintiffs had standing based on harm allegedly suffered by New Plaintiffs. This was improper because Town of Chester forbids a party from pointing to the injuries of another to establish his own standing. See also Spokeo, 136 S.Ct. at 1547 n.6 ("[N]amed plaintiffs who represent a 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."); In re SuperValu, Inc., 870 F.3d at 770-72 (fraud against one plaintiff did not create standing for other plaintiffs who were not victims of fraud).

Rehearing is needed to address these issues as well.

C. The Panel's Finding That Prior Plaintiffs Have Standing Directly Conflicts with Other Courts of Appeal.

The Court should also grant rehearing because the panel's holding that Prior Plaintiffs have standing, even though they did not allege any actual credit card

fraud or identity theft, directly conflicts with recent opinions by the Second, Fourth, and Eighth Circuits. See In re SuperValu, Inc., 870 F.3d at 770-72 (holding that one plaintiff who alleged credit card fraud had standing but the other 15 plaintiffs lacked standing because "data breaches are unlikely to result in account fraud"); Beck, 848 F.3d at 274 (plaintiffs lacked standing where, among other things, no named plaintiffs alleged misuse or their personal information and the theft had occurred some four years in the past); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (plaintiff lacked standing even though she alleged that thieves stole and attempted to use her credit card because plaintiff cancelled the credit card and was not liable for any fraudulent charges). Because the Supreme Court has not yet addressed what specific allegations are required for consumers to establish standing based on a hypothetically heightened risk of identity theft or fraud following a data breach, the panel's opinion substantially affects a rule of national application in which there is an overriding need for national uniformity. Importantly, in reaching its conclusion that standing was lacking, the Fourth Circuit relied on the persuasive analysis of the district court below. Beck, 848 F.3d at 275. The circuit split here is significant and stark. Rehearing *en banc* is warranted.

D. Rehearing Is Needed to Confirm That Clapper Overruled Krottner.

The Court should also grant rehearing *en banc* because the panel relied on authority that has been effectively overruled by the Supreme Court. In its opinion, the panel applied Krottner, 628 F.3d at 1142, which held that a "credible threat of harm" is sufficient to meet the injury in fact requirement for standing. See also id. ("the possibility of future injury may be sufficient to confer standing on plaintiffs").[6] But after Krottner, the Supreme Court adopted a different analysis and held that a "threatened injury must be *certainly impending* to constitute injury in fact and that allegations of *possible* future injury are not sufficient." Clapper, 133 S. Ct. at 1147 (emphasis in original).

"[C]ircuit precedent . . . can be effectively overruled by subsequent Supreme Court decisions that are closely on point, even though those decisions do not expressly overrule the prior circuit precedent." Miller v. Gammie, 335 F.3d 889, 899 (9th Cir. 2003) (citation omitted). Here, Clapper overruled Krottner because Clapper is closely on point. Specifically, in Clapper, the Supreme Court rejected the Second Circuit's "objectively reasonable likelihood" of future harm standard because it "is inconsistent with our requirement that threatened injury must be certainly impending to constitute injury in fact." 133 S. Ct. at 1147. Since Clapper, multiple courts have recognized that Krottner's "credible threat of harm"

[6] The district court found that Krottner requires both a "credible threat of harm" and that the harm be "certainly impending." (See ER 35-46.)

standard is inconsistent with Clapper. See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) (suggesting that Krottner was "thinly reasoned" and finding that it "is clearly not supportable" after Clapper); Duqum, 2016 WL 3683001, at *5 n.6 (distinguishing Krottner because it "predated Clapper and does not address or discuss either the 'certainly impending' standard or the 'substantial risk' standard"); Peters v. St. Joseph Servs. Corp., 74 F.Supp.3d 847, 855-56 (S.D. Tex. 2015) (recognizing the pre-Clapper circuit split but finding that Clapper "[a]rguably . . . resolved the circuit split" and "compels the conclusion" that plaintiffs lack standing to the extent the claims "are premised on the heightened risk of future identity theft/fraud").

Krottner's "credible threat of harm" standard is also inconsistent with the "substantial risk of harm" standard applied in Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2342 (2014). Indeed, a "substantial" risk of harm is more demanding than a "credible" risk of harm, but the panel used—without explanation—those two standards interchangeably in its opinion. (Compare Op. 12 (holding that Krottner's "credible threat" of harm standard controls) with id. 15 (finding that plaintiffs sufficiently alleged an injury in fact based on a "substantial risk" of harm).) Because the panel's opinion fuels uncertainty about the

appropriate standard to apply, and because it is inconsistent with Clapper, the Court should grant rehearing *en banc*.

IV. CONCLUSION

Accordingly, Zappos respectfully requests that the Court grant this Petition, order panel rehearing (or alternatively rehearing *en banc*), vacate the panel opinion, and issue a new and different opinion affirming the district court's order.

Dated: March 22, 2018

Respectfully submitted,

STROOCK & STROOCK & LAVAN LLP

By: */s/ Stephen J. Newman*
Julia B. Strickland
Stephen J. Newman
Brian C. Frontino
David W. Moon

KAEMPFER CROWELL
Robert McCoy

Counsel for Defendant-Appellee,
ZAPPOS.COM., INC.

EXHIBIT 1

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

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

Argued and Submitted December 5, 2017
San Francisco, California

Filed March 8, 2018

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

Opinion by Judge Friedland

SUMMARY**

Article III Standing

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

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

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

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

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

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

COUNSEL

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

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

OPINION

FRIEDLAND, Circuit Judge:

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

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

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

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

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

I.

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

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

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

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

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

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

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

II.

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

> a plaintiff must show (1) it has suffered an "injury in fact" that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

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

III.

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

A.

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

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

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

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

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

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

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

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

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

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

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

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

B.

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

C.

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

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

---

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

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

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

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

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

IV.

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

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

Form 11. Certificate of Compliance Pursuant to 9th Circuit Rules 35-4 and 40-1 for Case Number 16-16860

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the back of each copy of the petition or answer.*

I certify that pursuant to Circuit Rule 35-4 or 40-1, the attached petition for panel rehearing/petition for rehearing en banc/answer to petition (check applicable option):

☒ Contains 4,099 words (petitions and answers must not exceed 4,200 words), and is prepared in a format, type face, and type style that complies with Fed. R. App. P. 32(a)(4)-(6).

or

☐ Is in compliance with Fed. R. App. P. 32(a)(4)-(6) and does not exceed 15 pages.

Signature of Attorney or Unrepresented Litigant: s/ Stephen J. Newman

Date: Mar 22, 2018

("s/" plus typed name is acceptable for electronically-filed documents)

9th Circuit Case Number(s) 16-16860

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) Mar 22, 2018 .

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Signature (use "s/" format) s/ Stephen J. Newman

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)