No. 15-3690

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

DANIEL B. STORM, *et al.*,

Appellants,

v.

PAYTIME, INC., *et al.*,

Appellees.

On Appeal from the United States District Court
For the Middle District of Pennsylvania
Case No. 14-cv-1138
The Hon. John E. Jones III

PROPOSED BRIEF OF *AMICUS CURIAE* HORIZON HEALTHCARE SERVICES, INC. IN SUPPORT OF APPELLEES SEEKING AFFIRMANCE OF THE DISTRICT COURT'S RULINGS

David Jay
GREENBERG TRAURIG, LLP
500 Campus Drive, Suite 400
Florham Park, NJ 07932
(973) 360-7900
jayd@gtlaw.com

Kenneth L. Chernof
Arthur Luk
ARNOLD & PORTER LLP
601 Massachusetts Ave., NW
Washington, DC 20001
(202) 942-5000
ken.chernof@aporter.com
arthur.luk@aporter.com

Attorneys for Amicus Curiae Horizon Healthcare Services, Inc. d/b/a Horizon Blue Cross Blue Shield of New Jersey

May 23, 2016

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and Third Circuit Rule 26.1, *Amicus Curiae* Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey ("Horizon"), respectfully submits the following disclosure statement.

Horizon has no parent company and is not associated with any publicly held corporations. No publicly held corporation owns 10% or more of stock in Horizon.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

FEDERAL RULE OF APPELLATE PROCEDURE 29 STATEMENT

Pursuant to Rule 29(c)(4), Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey ("Horizon") states that, in accordance with Rule 29(b), it is concurrently filing a motion for leave to file this brief of *amicus curiae*.

Pursuant to Federal Rule of Appellate Procedure 29(c)(5), Horizon states that no party or counsel to any party in this matter authored this brief in part or in whole, no party or counsel to any party in this matter contributed money intended to fund the preparation or submission of this brief, and no person other than Horizon contributed money intended to fund the preparation or submission of this brief.

INTEREST OF *AMICUS CURIAE*

Amicus Curiae Horizon is Defendant-Appellee in a separate appeal pending before this Court: *In re Horizon Healthcare Servs. Inc. Data Breach Litig.* ("*In re Horizon"* or "*Horizon"*), No. 15-2309. *In re Horizon* was fully briefed and was scheduled for argument in January 2016; however, the Court temporarily held the case pending the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*. On May 16, 2016, the Supreme Court issued its decision in *Spokeo*, and on May 17, 2016, this Court directed the parties in *In re Horizon* to submit letters addressing the decision in *Spokeo* by May 31, 2016.

Horizon respectfully submits this *amicus curiae* brief in the case at bar ("*Paytime*") to (I) alert the Court to the similarities and differences between *Paytime* and *In re Horizon*; (II) amplify why there is no basis to overturn this Court's decision in *Reilly v. Ceridian Corp.*, 664 F.3d 28 (3d Cir. 2011); and (III) make clear that the Court should reject Appellants' blunderbuss approach, which, if credited, would establish standing in every purported "data breach" case.

ARGUMENT

I. *In re Horizon*

In re Horizon is the appeal of a putative class action in which the plaintiffs allege that their personal information may have been contained on two password-protected laptop computers that were stolen from Horizon by unknown thieves. *In re Horizon* is similar to *Paytime* in that both cases present issues relating to the

application of this Court's Article III standing decision in *Reilly*.[1] As in this case, the district court in *In re Horizon* dismissed the complaint because plaintiffs failed to allege the required concrete injury-in-fact fairly traceable to the defendant. *In re Horizon*, CV No. 13-7418 (CCC), 2015 WL 1472483, at *9 (D.N.J. Mar. 31, 2015). In doing so, the district court applied this Court's decision in *Reilly* and held that the plaintiffs did not plausibly allege that anyone accessed their data or suffered any concrete injury-in-fact as a result of the theft. *Id.* at *6 (finding plaintiffs suffered no actual harm and "conjectural" allegations about the "conduct of a third party" did not suffice). In Section II, below, we address why the Court should decline to overturn *Reilly*.

The cases are different, however, in at least two ways. *First*, the *Paytime* case involves only common-law claims, while the *Horizon* plaintiffs allege both common-law claims and a federal statutory claim for violation of the Fair Credit Reporting Act ("FCRA"). That difference led the *Horizon* plaintiffs to make the additional assertion that the availability of statutory damages allowed them to establish Article III standing even without actual injury. The district court rejected that argument, concluding that governing Third Circuit precedent requires a showing of concrete harm even when a federal statute permits statutory damages.

[1] Horizon's brief addresses these issues in detail. *See In re Horizon*, Appellee's Br. at 9-23.

Id. at *5. This is the issue that was before the Supreme Court in *Spokeo*, and the Supreme Court has now reached the same conclusion as the *Horizon* District Court: "Article III standing requires a concrete injury even in the context of a statutory violation." No. 13-1339, —S. Ct. —, 2016 WL2842447, at *7 (May 16, 2016). But this issue is not presented in *Paytime*.

Second, *In re Horizon* involves a garden-variety theft of laptop computers, whereas *Paytime* involves an alleged targeted hacking incident. To be sure, controlling Supreme Court and Third Circuit jurisprudence makes clear that standing cannot be established in either case, because none of the plaintiffs alleged plausible evidence of concrete injury fairly traceable to the incident. *See* Section II, below. But the differing fact patterns between the *Horizon* and *Paytime* cases—as well as the many other kinds of "data breach" cases—illustrate why it is important for the Court to decline Appellants' sweeping invitation to find standing for anything labeled a "data breach" alleged to have been committed for a "nefarious purpose." Appellants' Br. at 16. *See* Section III, below.

II. *Reilly* Controls and Should Not Be Overturned

This Court's 2011 decision in *Reilly* mandates dismissal of *Paytime* for lack of standing, which is why Appellants and *Amicus Curiae* Electronic Privacy Information Center ("EPIC") directly or indirectly ask that the Court overturn it. EPIC candidly concedes that overturning *Reilly* is precisely what it seeks (*see*

EPIC Br. at 2), while Appellants propose an interpretation of *Reilly* that would strip its holding bare. Appellants' Br. at 28-33. *Reilly*, however, is a binding opinion of this Court, as the Third Circuit's rules and precedent make clear.[2] But even if the Court could overrule *Reilly*, Appellants and EPIC have provided no reason why it should do so.

Reilly involved a situation in which a hacker "infiltrated [the defendant's] system and potentially gained access to personal and financial information." 664 F.3d at 40. Despite the plaintiffs' contentions that the hacker "intend[ed] to commit future criminal acts by misusing the information," this Court upheld the district court's dismissal for lack of Article III standing because "Appellants' allegations of hypothetical, future injury are insufficient to establish standing." *Id.* at 42. Rather, for a future injury to satisfy Article III, the "threatened injury must be certainly impending." *Id.* (internal quotation marks omitted). Furthermore, this Court made clear that a "string of hypothetical injuries do not meet the requirement of 'actual or imminent' injury" for Article III standing. *Id.* at 44. This Court

---

[2] *See* Internal Operating Procedures of the United States Court of Appeals for the Third Circuit, Chapter 9.1 (effective 2015), http://www2.ca3.uscourts.gov/legacyfiles/2015_IOPs.pdf ("It is the tradition of this court that the holding of a panel in a precedential opinion is binding on subsequent panels. Thus, no subsequent panel overrules the holding in a precedential opinion of a previous panel"); *O. Hommel Co. v. Ferro Corp.*, 659 F.2d 340, 354 (3d Cir. 1981) ("[A] panel of this court cannot overrule a prior panel precedent," and so "[t]o the extent that it is inconsistent with [an older decision], [the new decision] must be deemed without effect").

explained: "In this increasingly digitized world, a number of courts have had occasion to decide whether the 'risk of future harm' posed by data security breaches confers standing on persons whose information *may* have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative. *We agree with the holdings in those cases*." *Id.* at 43 (citations omitted) (second emphasis added).[3]

Reilly is squarely on point and mandates dismissal for lack of standing. And it was clearly correct. As an initial matter, it was consistent with the great weight of existing precedent at the time it was decided less than five years ago,[4] and it carefully and thoughtfully distinguished the few inconsistent and poorly reasoned out-of-circuit decisions. *Reilly*, 664 F.3d at 43-46. And in the years since it was

[3] EPIC also argues that this Court should overturn its holding in *Reilly* because a mere five years ago this Court could not have understood "the problem of identity theft." EPIC Br. at 1. Not only is this inaccurate, it is contradicted by the well-reasoned opinion in *Reilly*, where the Court made clear that it understood data breaches in "this increasingly digitized world." *Reilly*, 664 F.3d at 43.

[4] *See Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) ("[B]ecause [the plaintiff] does not identify any incident in which her data has ever been accessed by an unauthorized person, she cannot satisfy Article III's requirements of actual or impending injury."); *Allison v. Aetna, Inc.*, No. 09-CV-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-CV-6060, 2010 WL 2643307, at *6-8 (S.D.N.Y. June 25, 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052-53 (E.D. Mo. 2009); *Bell v. Acxiom Corp.*, No. 06-CV-485, 2006 WL 2850042, at *1-2 (E.D. Ark. Oct. 3, 2006); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006); *Giordano v. Wachovia Sec., LLC*, No. 06-CV-476, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006); *cf. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164-65 (1st Cir. 2011) (finding injury only where "there was actual misuse" of credit and debit card data targeted by hackers, and distinguishing "theft of expensive computer equipment" cases where there is no identity theft and no allegation that thieves targeted personal information).

decided, *Reilly* and/or its reasoning have been followed and applied by the vast majority of similar cases that have come in its wake.[5]

Importantly, the Supreme Court has confirmed the propriety of this Court's *Reilly* analysis. In *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), the Supreme Court held—just as *Reilly* did—that in order for Article III standing to be based on the potential for future harm, the allegedly "threatened injury must be

[5] *See In re Horizon*, 2015 WL 1472483, at *5 ("The Third Circuit's decision in *Reilly* is both squarely on point and binding on this Court. . . . Simply put, 'there [was] no misuse of the information, and thus, no harm.'" (quoting *Reilly*, 664 F.3d at 42)); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 470-71 (D.N.J. 2013) (relying on *Reilly* and *Clapper* in dismissing case arising out of theft of laptop containing medical information for lack of standing in absence of actual misuse of information); *see also Alonso v. Blue Sky Resorts, LLC*, —F. Supp. 3d—, 2016 WL 1535890, at *5 (S.D. Ind. Apr. 14, 2016) (finding "any future harm . . . highly speculative" when there existed "no evidence (or allegations) of actual fraudulent activity ever occurring"), *appeal docketed*, No. 16-2136 (7th Cir. May 16, 2016); *Whalen v. Michael Stores Inc.*, —F. Supp. 3d—, 2015 WL 9462108, at *5 (E.D.N.Y. Dec. 28, 2015) (relying on *Clapper* to dismiss because plaintiff failed to allege a certainly impending injury or a substantial risk of harm), *appeal docketed*, No. 16-260 (2d Cir. Jan. 27, 2016); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014) (holding that the risk of identity theft is insufficient to constitute injury in fact for purposes of standing); *Galaria v. Nationwide Mut Ins. Co.*, 998F. Supp. 2d 646, 654 (S.D. Ohio 2014) (relying on *Clapper* to hold that "an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—or offer facts to make plausible—an allegation that such harm is 'certainly impending'"); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) (relying on *Clapper* to hold that increased risk of identity theft insufficient to confer standing); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("*Clapper* compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing"); *Peters v. St. Joseph Svcs. Corp.*, 74 F. Supp. 3d 847, 855-56 (S.D. Tex. Feb. 11, 2014) (holding that an increased risk of future identity theft or fraud is insufficient to confer Article III standing); *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531, at *6 (E.D. La. May 4, 2015) (dismissing data breach case for lack of standing where no actual identity theft or fraud was alleged); *In re Zappos.com, Inc.*, *Customer Data Security Breach Litig.*, 108 F. Supp. 3d 949, 958-59 (D. Nev. 2015) (finding 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").

c*ertainly impending* to constitute an injury in fact" and "[a]llegations of *possible* future injury are not sufficient." *Id.* at 1147 (internal quotation marks omitted); *see also Spokeo*, 2016 WL 2842447, at *8 (citing *Clapper* on when a risk of harm can "satisfy the requirement of concreteness.")

The Court should therefore decline the invitation by Appellants and EPIC to rely on *Remijas v. Neiman Marcus*, 794 F.3d 688 (7th Cir. 2015) and *In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014). To the extent they permit standing without a showing that future injury is "certainly impending," those decisions are inconsistent with *Clapper* and *Reilly* and wrongly decided. Indeed, the finding in *Remijas* that an "objectively reasonable likelihood" of a future injury satisfies Article III standing, 794 F.3d at 693, was expressly rejected by the Supreme Court, which instead mandated that a future injury must be certainly impending, *Clapper*, 133 S. Ct. at 1147 ("[The] 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.'"). This Court rejected cases with similarly "skimpy rationale" regarding Article III standing in *Reilly*, and it should do so again here. *Reilly*, 664 F.3d at 44.[6]

[6] Moreover, both *Remijas* and *Adobe* are plainly distinguishable on their facts because in both cases the courts found undisputed evidence that some individuals had already experienced actual misuse of their personal information that was fairly traceable to the data breach. *See Remijas*, 794 F.3d at 692 (9,200 individuals had already incurred fraudulent charges); *In re Adobe*, 66 F. Supp. 3d at 1215 ("Some

Footnote continued on next page

III. A "Data Breach" Does Not Automatically Confer Article III Standing

As EPIC admits: "Not all data breaches are created equal. Some breaches are the result of highly sophisticated attacks carried out by anonymous hackers, while others involve physical theft of computers or storage devices containing sensitive records." EPIC Br. at 10. Yet the holding that Appellants and EPIC seek would create Article III standing whenever an incident potentially involves personal information. According to Appellants, all a plaintiff must do is describe the motive of the thief as "nefarious" in order to satisfy Article III standing. Appellants' Br. at 16. This would be the case despite the great variation in types of incidents EPIC generally categorizes as "data breaches," and—most importantly—regardless of whether there is plausible evidence of actual injury. Labeling any attack as "nefarious" is simply not a substitute for alleging the plausible evidence of concrete injury mandated by this Court in *Reilly* and the Supreme Court in *Clapper*.

For example, the allegations in *In re Horizon* involve the theft of two password-protected laptops. But the mere allegation of stolen hardware—without plausible allegations that the thieves knew what the devices contained, had accessed the information, or could access the information, much less had used the

Footnote continued from previous page
of the stolen data has already surfaced on the Internet, and other hackers have allegedly misused it to discover vulnerabilities in Adobe's products.").

information—is plainly insufficient to establish concrete injury. *See In re Horizon*, 2015 WL 1472483, at *9 (dismissing because "none of the named Plaintiffs have adequately alleged Article III standing"); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015) (rejecting plaintiff's argument that the theft of backup data tapes caused an increased risk of injury because it required the court to speculate about the thief's capabilities of accessing the information contained); *In re SAIC*, 45 F. Supp. 3d at 25 (rejecting plaintiffs' increased risk of harm argument based on the theft of backup data tapes and noting that until there was actual misuse, there was no way of knowing whether the personal information contained on the tapes was even accessed). Thefts happen all the time and, given the ubiquity of electronic devices, will frequently involve devices that may contain personal information. The Court should not hold that these sorts of garden-variety crimes automatically create a viable federal lawsuit based on a perceived "risk" of identity theft for anyone whose data might have been on a stolen device.

To do so would be contrary to the decisions of this Circuit and the Supreme Court, which have expressly held that Article III permits standing only where a plaintiff can plausibly allege they have suffered a present injury or that concrete injury is not just "possible" but rather "certainly impending." *Clapper*, 133 S. Ct. at 1147 (holding that even an "objectively reasonable" fear of future harm is insufficient to establish standing); *Reilly*, 664 F.3d at 42.

These principles foreclose Appellants' standing in the case at bar as well as their attempt to manufacture standing in any "data breach" case where they allege some third party's bad intent. The Supreme Court said it plainly and with emphasis: "[a]llegations of *possible* future injury are not sufficient." *Clapper*, 133 S. Ct. at 1147 (internal quotation marks omitted).

CONCLUSION

The judgment of the district court should be affirmed.

Dated: May 23, 2016

Respectfully submitted,

/s/ Kenneth L. Chernof

Kenneth L. Chernof
Arthur Luk
ARNOLD & PORTER LLP
601 Massachusetts Ave., NW
Washington, DC 20001
(202) 942-5000
ken.chernof@aporter.com
arthur.luk@aporter.com

David Jay
GREENBERG TRAURIG, LLP
500 Campus Drive, Suite 400
Florham Park, NJ 07932
(973) 360-7900
JayD@gtlaw.com

Attorneys for Amicus Curiae Horizon Healthcare Services, Inc. d/b/a Horizon Blue Cross Blue Shield of New Jersey

CERTIFICATE OF COMPLIANCE

I certify, pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Third Circuit Rule 31.1(c), that the attached Brief of *Amicus Curiae*:

(1) contains 3955 words;

(2) complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font; and

(3) has been scanned for viruses using Microsoft System Center Endpoint Protection (Antimalware Client Version 4.6.305.0 & Engine Version 1.1.12101.0) and is free from viruses.

I further certify that the text of the electronic brief is identical to the text in the paper copies.

/s/ Kenneth L. Chernof
Dated: May 23, 2016 Kenneth L. Chernof

Attorney for Amicus Curiae Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey

CERTIFICATE OF BAR MEMBERSHIP

I certify, pursuant to Third Circuit Rule 28.3(d), that I am a member of the Bar of this Court.

Dated: May 23, 2016

/s/ Kenneth L. Chernof
Kenneth L. Chernof

CERTIFICATE OF SERVICE

I hereby certify that on May 23, 2016, I electronically filed the foregoing *Brief of Amicus Curiae* with the Clerk of the Court for the United States Court of Appeals for the Third Circuit via the Court's appellate CM/ECF system. Participants in the case who were registered CM/ECF users were served by the CM/ECF system at that time.

Further, I hereby certify that on May 23, 2016, I served 7 paper copies on the Clerk of the Court for the United States Court of Appeals for the Third Circuit via Federal Express Priority Overnight.

Dated: May 23, 2016

/s/ Kenneth L. Chernof
Kenneth L. Chernof