Legal Backgrounder

Vol. 30 No. 30 December 11, 2015

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Seventh Circuit's *Neiman Marcus* Data-Security Ruling Breaches Standing Jurisprudence

by Evan A. Young

As recently as 2013, the U.S. Supreme Court reemphasized the "well-established requirement" that, for plaintiffs to establish Article III standing regarding threatened (rather than present) injury, they must show that the injury is "certainly impending."[1] Whether using that particular formulation or others, such as a showing of "substantial risk,"[2] the Court's goal has been to prevent the erosion of the fundamental principle that *actual injury* is an essential prerequisite to the exercise of Article III power. In the past few years, numerous district courts have applied the "certainly impending" standard in the context of data breaches where hackers steal consumers' personal information en masse, and most have held that plaintiffs do not establish standing when harm resulting from the breach through fraudulent charges or identity theft has not yet occurred.[3] But a recent Seventh Circuit decision, *Remijas v. Neiman Marcus Group, LLC*,[4] bucks that trend and threatens to dial back standing requirements in data-breach cases, thus potentially greenlighting enormous class-action suits without any showing of non-speculative harm.

In *Remijas*, the named plaintiffs brought a class action alleging harm based upon a 2013 cyberattack on Neiman Marcus, a luxury department store. "[A]pproximately 350,000 [debit or credit] cards had been exposed to the hackers' malware," those 350,000 customers' "data may have been hacked," and they therefore were "potentially exposed" to fraud and identity theft.[5] Neiman Marcus notified its customers and offered to anyone who shopped at its stores between January 2013 and January 2014 a year of free credit monitoring and identity-theft protection.[6] Of the 350,000 "potentially exposed" cards, 9,200 were known to

---

[1] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013).
[2] *Id.* at 1150 n.5.
[3] *E.g.*, *Fernandez v. Leidos, Inc.*, __ F. Supp. 3d __, No. 2:14-cv-02247-GEB-KJN, 2015 WL 5095893 (E.D. Cal. Aug. 28, 2015) (appeal filed); *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359 (M.D. Pa. 2015); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014); *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871 (N.D. Ill. 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013). *But see In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (concluding that plaintiffs gained standing by threatened injury from data breach); *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (same); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (same).
[4] 794 F.3d 688 (7th Cir. 2015).
[5] *Id.* at 690.
[6] *Ibid.*

Evan A. Young is a Partner with Baker Botts LLP in its Austin, Texas office, where he serves as Litigation Department chair. Special thanks go to **Jonathan Levy** for his thoughtful and invaluable assistance.

have actually been used fraudulently, albeit without any evidence of identity theft.[7] "Notably," the Seventh Circuit added, "other companies had also suffered cyberattacks during that holiday season."[8] The district court ruled that no plaintiff from either group—the 9,200 or the remainder of the 350,000—had standing, and accordingly dismissed the case without prejudice.

The Seventh Circuit reversed. It began by acknowledging that establishing standing is the plaintiffs' burden and that they "must allege that the data breach inflicted concrete, particularized injury on them; that Neiman Marcus caused that injury; and that a judicial decision can provide redress for them."[9] The court also held that the 9,200 fraud victims, though they were later reimbursed for all fraudulent charges, established standing because of the "identifiable costs associated with the process of sorting things out."[10]

More importantly, however, it reached the same result for the rest of the 350,000 plaintiffs—those who were only potentially susceptible to future harm as a result of the breach.[11] Treating the two groups as effectively identical, the court found standing for all plaintiffs by (1) distinguishing this case from *Clapper*, because (it said) the future harm in *Clapper* was more attenuated and speculative; (2) warning that requiring plaintiffs to wait until they are actually harmed would afford defendants more latitude to assert that there is no causal connection between the breach and the harm; (3) inferring that because the presumed purpose of a cyberattack is to make fraudulent charges and steal identities, the risk of such harm occurring was substantial; and (4) reasoning, "It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection. . . . It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."[12]

Each of these rationales for the as-yet-unharmed plaintiffs' standing is questionable at best. First, *Remijas* certainly arose from different facts than *Clapper*, but that does not justify less skepticism or rigor about standing here. In *Clapper*, the Court held that the harm alleged—likely future surveillance of the plaintiffs' communications under Section 1881a of the Foreign Intelligence Surveillance Act (FISA)—was too speculative.[13] The Supreme Court noted that standing would have depended upon a long "speculative chain of possibilities,"[14] because each of the following would have to happen for the alleged harm to actually occur: (1) the government imminently targets communications to which the plaintiffs are parties; (2) the government seeks authorization of surveillance under Section 1881a of FISA; (3) the court authorizes such surveillance; (4) the government succeeds in acquiring the communications of the plaintiffs' foreign contacts; and (5) the plaintiffs' own communications with their foreign contacts are acquired.[15] In data breach cases, too, the unknowns are legion. As one court put it,

> Whether [the plaintiffs] actually become victims of identity theft as a result of the data breach depends on a number of variables, such as whether their data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded. . . .

[7] *Id.* at 690, 692.
[8] *Id.* at 690.
[9] *Id.* at 691–92.
[10] *Id.* at 692. At least two courts have held that reimbursed charges are insufficient to confer standing in this context. *See Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014) (appeal filed); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279 (N.D. Ala. 2014).
[11] *Remijas*, 794 F.3d at 694. The court's conflation of the two groups is notable.
[12] *Id.* at 693–94. The court also expressed doubt that, but did not decide whether, the plaintiffs' other asserted injuries—lost money from overpaying at Neiman Marcus and lost value of personal information—conferred standing. *Id.* at 694–96.
[13] 133 S. Ct. at 1143.
[14] *Id.* at 1150.
[15] *Id.* at 1148–50.

> Like the plaintiffs in *Clapper*, the harm that [the plaintiffs] fear[] is contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendant.[16]

The Seventh Circuit warned in *Remijas* that "it is important not to overread *Clapper*," and noted that there was "no need to speculate as to whether [the Neiman Marcus customers'] information ha[d] been stolen and what information was taken."[17] Fair enough. But the *Remijas* opinion commits the opposite error of *under*reading *Clapper*, by focusing on only one step when *Clapper* concerned an attenuated *chain* of speculative steps. Even accepting that the *Remijas* plaintiffs' data were compromised, in other words, would (at best) remove one obstacle to showing harm sufficient for standing. The plaintiffs still could not "describe how [they] will be injured without beginning the explanation with the word 'if,'"[18] and as such, meeting *Clapper*'s "certainly impending" requirement, or indeed even a lesser articulation of it, would be challenging.[19]

Second, even supposing that data-breach defendants would have more leverage to argue against causation if plaintiffs must wait until actual harm occurs, that says nothing about whether a currently unrealized harm is too speculative to satisfy standing's *injury-in-fact* requirement.[20] And indeed, the real significance of the ability to project actual harm from data breaches to a future time is not that the defendant may contest causation, but rather that the possible harm is not "certainly impending" to begin with.[21]

Third, even assuming that the hackers intended to commit fraud and identity theft, the risk to any given plaintiff may not be substantial.[22] In many cases, plaintiffs' lawyers have cited studies indicating that data-breach victims are 9.5 times more likely than others to become victims of fraud or identity theft, but courts have consistently rejected that argument, concluding that relative likelihood is irrelevant to whether the risk of future harm is substantial in and of itself.[23] In addition, the purpose of insisting that a future harm be "certainly impending" to establish standing, or that the risk of that harm be substantial, is "to reduce the possibility of deciding a case in which no injury would have occurred at all."[24] If mere statistical likelihood of harm sufficed, the requirement of *actual* harm would be largely erased, and many Supreme Court standing cases would be effectively overruled.[25] And in any event, if a court decides a case as to a data-breach victim who has not yet suffered harm, there is in fact a *two-thirds* chance that the court will have thwarted that purpose.[26] Whatever probability of harm is required to be "substantial," it is doubtful that this qualifies.

---

[16] *Strautins*, 27 F. Supp. 3d at 876.

[17] 794 F.3d at 693–94 (first alteration in original) (quoting *Adobe Sys.*, 66 F. Supp. 3d at 1215).

[18] *Peters*, 74 F. Supp. 3d at 854 (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011)).

[19] *See Clapper*, 133 S. Ct. at 1150 n.5.

[20] In a separate part of the *Remijas* opinion, the court held that because it was at least plausible that the plaintiffs' injuries were traceable to the Neiman Marcus breach, the plaintiffs met the (distinct) causation requirement for standing at the pleading stage. 794 F.3d at 696.

[21] *See Clapper*, 133 S. Ct. at 1160 (Breyer, J., dissenting) (discussing cases in which the Court denied standing because the future harm was too remote temporally).

[22] *Clapper* admits of a "substantial risk" formulation for assessing whether a future injury confers standing, but does not decide whether that standard is distinct from the "certainly impending" formulation. 133 S. Ct. at 1150 n. 5. In any event, for reasons discussed here, a data-breach victim who has not yet suffered harm does not meet either standard.

[23] *See, e.g.*, *Green*, 2015 WL 2066531, at *5; *Sci. Applications*, 45 F. Supp. 3d at 25; *Strautins*, 27 F. Supp. 3d at 877; *Galaria*, 998 F. Supp. 2d at 654.

[24] *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 564 n.2.

[25] *See, e.g.*, *Summers v. Earth Island Inst.*, 555 U.S. 488 (2009) (denying standing despite affidavit that plaintiff had visited and planned to visit substantial areas subject to challenged regulations without identifying a specific location).

[26] *See* Catey Hill, *Fraud Hits One in Three Data-Breach Victims*, MarketWatch (Feb. 6, 2014, 7:49 AM), http://www.marketwatch.com/story/fraud-hits-one-in-three-data-breach-victims-2014-02-05 (noting that "in 2013, one in three consumers who received a data-breach notification became a victim of fraud").

ISBN 1056 3059

Finally, by treating Neiman Marcus's offer of free credit monitoring and identity-theft protection as an admission that the risk of future harm is more than "ephemeral,"[27] the Seventh Circuit's opinion threatens to chill a common, consumer-friendly practice among data-breach defendants. While offering free protection in such cases is par for the course,[28] it is not unheard of that a company will decline to do so.[29] If potential defendants decline to offer protection because it is effectively treated as an admission, consumers and defendants would both suffer—consumers would have to incur out-of-pocket expenses to protect against possible harm, and defendants would find that a means of dispute resolution has become fuel for the litigation fire instead.[30]

Perhaps what is most troubling about *Remijas* is the Seventh Circuit's apparent certainty in concluding that none of this even poses an Article III problem, despite openly acknowledging most of the 350,000 plaintiffs to have only potential "future injuries."[31] Courts should be cautious about pressing the boundaries of Article III, which (at least under current Supreme Court precedent) exists in large part to ensure that the judicial power of the United States is invoked only to resolve actual injuries. The fact pattern in this case is certainly sympathetic; no one relishes having one's financial and personal information exposed to unauthorized recipients, regardless of whether one is ever ultimately injured. But it is in sympathetic cases that fundamental values can be most easily eroded, and where they must therefore be most deliberately protected.[32] Other courts should give the question of standing presented in *Remijas* more scrutiny and skepticism than the Seventh Circuit did.

---

[27] The court's phrasing betrays its misapplication of the *Clapper* standard, which requires far more than that the risk of harm be "not ephemeral." Case in point, the court reasons that "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." *Remijas*, 794 F.3d at 693 (quoting *Clapper*, 133 S. Ct. at 1147). In fact, the Supreme Court rejected an "objectively reasonable likelihood" standard because it is "inconsistent with [the Court's] requirement that 'threatened injury must be certainly impending to constitute injury in fact.'" *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

[28] *E.g.*, *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, No. 13-7418 (CCC), 2015 WL 1472483, at *5 (D.N.J. March 31, 2015) (appeal filed); *Peters*, 74 F. Supp. 3d at 850; *Adobe Sys.*, 66 F. Supp. 3d at 1207; *Moyer*, 2014 WL 3511500, at *2; *SAIC*, 45 F. Supp. 3d at 20; *Strautins*, 27 F. Supp. 3d at 881; *Galaria*, 998 F. Supp. 2d at 650; *Sony*, 996 F. Supp. 2d at 955.

[29] *E.g.*, *In re Zappos.com, Inc.*, __ F. Supp. 3d __, No. 3:12-cv-00325-RCJ-VPC, 2015 WL 3466943, at *10 n.4 (D. Nev. June 1, 2015).

[30] Indeed, within two months of the *Remijas* opinion, plaintiffs' lawyers already used this argument against a defendant in at least two cases. *See* Plaintiffs-Appellants' Brief at 18, *Galaria v. Nationwide Mut. Ins. Co.*, Nos. 15-3386, 15-3387 (6th Cir. Sept. 18, 2015) ("Nationwide acknowledged the significant risk of harm faced by Plaintiffs and the other Victims in offering a free year of credit monitoring and identity theft protection. As [*Remijas*] notes, '[i]t is unlikely that [a defendant offers credit monitoring protection] because the risk is so ephemeral that it can safely be disregarded.'" (second and third alterations in original) (citation omitted) (quoting *Remijas*, 794 F.3d at 694)); Opening Brief of Appellants at 31–32, *Beck v. Shinseki*, Nos. 15-1395, 15-1715 (4th Cir. Aug. 10, 2015) (arguing that "the Secretary [of Veterans Affairs]' decision to expend federal funds [on mitigation actions] makes it similarly 'unlikely' that the risk was ephemeral" (quoting *Remijas*, 794 F.3d at 694)).

[31] 794 F.3d at 694.

[32] After all, the Judiciary is not the only branch of government capable of dealing with allegations of commercial wrongs. The other branches can probe such allegations and impose consequences, even when no particular individual plaintiff has standing to seek a private remedy.

  ISBN 1056 3059