Seventh Circuit Finds Article III Standing for Data Breach Class Action Based on Allegations of Future Harm

By Joseph R. Tiffany II and Connie J. Wolfe, Ph.D.

In the wake of numerous data breach cases dismissed for lack of Article III standing based on the Supreme Court's decision in Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013), the Seventh Circuit Court of Appeals has become the first post-Clapper appellate court to hold that data breach victims adequately alleged standing based on risks of future harm. In* Remijas v. Neiman Marcus Group, LLC*, --- F.3d ----, 2015 WL 4394814, Case No. 14-3122 (7th Cir. July 20, 2015) ("*Remijas*"), the district court dismissed a class action complaint against retailer Neiman Marcus based on the plaintiffs' lack of Article III standing. Plaintiffs appealed, and the Seventh Circuit reversed. The decision adds a new element of uncertainty for custodians of customer data impacted by data breaches.*

The *Remijas* complaint arose from a cyberattack in 2013, in which data for approximately 350,000 payment cards was potentially exposed to hacker malware. Fraudulent use was reported on 9,200 (approximately 2.6 percent) of the potentially exposed cards. The plaintiffs alleged, among other things, "imminent injuries" based upon an increased risk of future fraudulent charges and greater susceptibility to identity theft.

In an opinion written by Chief Judge Wood, the Court first considered whether plaintiffs' "imminent injury" allegations satisfied the standard established in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013), that harm must be "certainly impending."[1] The Seventh Circuit noted that the *Clapper* decision did not eliminate the possibility of finding standing based on "a 'substantial risk' that the harm will occur."[2] In *Clapper*, the Supreme Court held that human rights organizations and media groups who challenged the

[1] Id. at *3

[2] Id. at *4

Foreign Intelligence Surveillance Act of 1978 on the ground that their confidential communications would be subject to surveillance lacked Article III standing.[3] The Court distinguished *Clapper*, noting that plaintiffs in that case "could not show that their communications with suspected terrorists were intercepted by the government," but only that they "suspected that such interceptions *might have* occurred"[4] (emphasis added).

The case law regarding standing for data breach claims has varied between jurisdictions before and after *Clapper*:

> Pre-*Clapper*, both the Ninth and Seventh Circuits found injury-in-fact based on increased risk of future harm in data breach cases. *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding threat of harm injury based on allegations of attempted identity theft following targeted theft of laptops containing unencrypted personal data); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (finding injury based on threat of future harm when "the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious."). In contrast, the Third and First Circuits held that alleged threats of future harm were insufficient to establish standing. *Reilly v. Ceridian Corp*., 664 F.3d 38, (3d Cir. 2011) (finding no injury-in-fact absent evidence of data misuse or any "identifiable taking" following a firewall breach); *Katz v. Pershing, LLC*, 672 F.3d 64, 79-80 (1st Cir. 2012) (finding no injury-in-fact when plaintiff's claim was based on defendant's allowing a service provider access to plaintiff's personal data which she alleged could lead to unauthorized access and increased risks of identity theft).
>
> Post-*Clapper*, a number of district courts have refused to find Article III standing based on threats of future harm in data breach cases. *See, e.g., Peters v. St. Joseph Services Corp.*, 74 F.Supp.3d 847, 854 (S.D. Tex. 2015) (holding that increased risk of future identity theft or fraud based on data breach was not a cognizable Article III injury); *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 26 (D.D.C. 2014) (holding that allegations of potential future identity theft based on actions of an unknown third party were insufficient to establish standing); *Galaria v. Nationwide Mut. Ins. Co.,* 998 F.Supp.2d 646, 654 (S.D.Ohio 2014) (holding that allegations that plaintiffs' personal information was stolen and disseminated were insufficient to establish standing when plaintiffs did not allege that their data had been misused). *But see In re Adobe Sys., Inc. Privacy Litig*.,66 F.Supp.3d 1197, 1214 (N.D. Cal. 2014) (finding standing where hacker spent several weeks collecting sensitive customer information).

In *Remijas*, the Court found that the circumstances were similar to those of *Adobe*, in which plaintiffs alleged a deliberate hacker attack and the district court found the risk that plaintiffs' personal data would be used by the hackers "is immediate and very real."[5] In *Adobe,* the data accessed by hackers included customer "names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses."[6] The Court pointed to plaintiffs' allegations that hackers had "deliberately targeted Neiman Marcus in order to obtain their credit-card information" and that 9,200 cards had "experienced fraudulent charges *so far*"[7] (emphasis in original). The Court further noted that a government report cited by plaintiffs found that stolen data may be held for up to a year or more before initial use, and then may be used for

[3] Id.

[4] Id.

[5] *Remijas*, 2015 WL 4394814 at *4.

[6] *In re Adobe Sys*., 66 F.Supp.3d at 1206.

[7] Id. at *4-5

years thereafter.[8] Based on such allegations, the Court found "it is plausible to infer that the plaintiffs have shown a substantial risk of harm" at the pleading stage, but recognized that they might not be able to provide an adequate factual basis for the inference as the case proceeds.[9]

Plaintiffs further alleged several types of actual harm: (1) lost time and injury resolving the fraudulent charges; (2) lost time and money protecting themselves against future identity theft; (3) overcharges for Neiman Marcus products that they would not have purchased if they had known of the store's inadequate cybersecurity; and (4) lost control over the value of their personal information.[10] The Court quickly disposed of the defendant's challenge to the standing of plaintiffs who had been exposed to fraudulent charges, agreeing with the plaintiffs "that there are identifiable costs associated with the process of sorting things out."[11] The Court further held that plaintiffs had adequately alleged lost time and money protecting against future identity theft and fraudulent charges.[12] The Court characterized such mitigation expenses as addressing more than "speculative" harm, as it was undisputed that the breach occurred, Neiman Marcus itself offered credit monitoring and identity-theft protection implying a non-ephemeral concern, and the costs of such services were not *de minimis*.[13] The Court refrained from deciding the sufficiency of the last two categories of harm, but noted that it was "dubious" that such alleged injuries were sufficient to establish standing on their own.[14] Regarding the alleged overcharge injuries, the Court found that the plaintiffs' theory based on product liability and unjust enrichment required "a step that we need not, and do not, take in this case."[15] Finding no authority to support plaintiffs' allegation of harm due to loss of control of personal data, the Court refrained from deciding whether such allegations might suffice as injuries for Article III standing.[16]

The Court further found that plaintiffs adequately pleaded the remaining prerequisites for Article III standing: causation and redressability.[17] The Court found that the allegations of injury were "fairly traceable" to the hacker attack, as it was enough at the pleading stage that the defendant admitted that 350,000 cards might have been exposed and that it had contacted card members to tell them of the risk.[18] The Court also held that the injuries were redressable because payment card reimbursement policies may vary, and all mitigation expenses and potential future injuries may not be fully reimbursed without Court action.[19]

The *Remijas* decision raises serious concerns for retailers and other holders of personal customer data. The Court pointed to the Neiman Marcus offer of a year of free credit-monitoring services as "telling" evidence that future harm was not ephemeral and speculative, yet failed to address why additional mitigation would be necessary after such services were provided.[20] Following *Remijas*, companies suffering

[8] Id. at *5

[9] Id.

[10] Id. at *3-4

[11] Id. at *4

[12] Id. at *5

[13] Id.

[14] Id. at *6-7

[15] Id. at *6. Notably, the issue of Article III standing based on a similar "overpayment theory" and other allegations is currently on appeal in the 8th Circuit in the context of data sharing by a gaming services provider. *See Carlsen v. GameStop, Inc*., Case No. 14-3131, 2015 WL 3538906 (Minn. 2015), appealed to the 8th Circuit, Case No. 15-2453 (opening brief due September 25,2015).

[16] Id.

[17] Id. at *7

[18] Id.

[19] Id. at *8

[20] Id. at *5

future data breaches will have to consider the risk that offering credit monitoring services to their customers, which has become standard for companies suffering data breach incidents, may subject them to a similar adverse inference of future injury sufficient to establish standing.

Neiman Marcus has recently petitioned for rehearing en banc, asserting that the *Remijas* opinion "squarely conflicts" with the holding in *Clapper* requiring "imminent" and "certainly impending" harm to establish Article III standing. It remains to be seen whether the case will be reviewed en banc and, if not, whether future cases will limit the *Remijas* holding to the facts of this case, in which the breach allegedly arose from a deliberate hacker attack and significant numbers of potentially exposed cards were subject to fraudulent charges, or whether it will be extended to apply to other hacker-breach cases, regardless of documented fraud. In any event, the holding is one more reminder of the need to remain vigilant in the protection of customer information, and to take quick action upon discovery of any breach.

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Joseph R. Tiffany II **(bio)**
Silicon Valley
+1.650.233.4644
joseph.tiffany@pillsburylaw.com

Connie J. Wolfe, Ph.D. **(bio)**
San Diego
+1.619.544.3139
connie.wolfe@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.