Supplement to the Los Angeles and San Francisco
Daily Journal
JANUARY 23, 2019

TOP CYBER LAWYERS

New York Times News Service

The U.S. Supreme Court building in Washington, D.C. There is a substantial split among the circuit courts regarding the appropriate standard for finding Article III standing in cybersecurity class actions. The conflict cries out for high court resolution and compels companies and their lawyers to think strategically about ways to handle — and avoid — cybersecurity litigation.

Circuit split underscores the need for strategic thinking in defending cybersecurity class actions

By Ian C. Ballon

There is currently a substantial circuit split on the appropriate standard for finding Article III standing in putative cybersecurity breach class actions. The 6th, 7th, 9th and D.C. Circuits have set a lower bar for what satisfies the requirements for Article III standing in a cybersecurity case than the 2nd, 3rd, 4th and 8th Circuits. The conflict among the circuits cries out for Supreme Court resolution and compels companies and their lawyers to think strategically about ways to handle — and avoid — cybersecurity litigation. To sue in federal court, a plaintiff must establish standing within the meaning of Article III of the U.S. Constitution. To do so, a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision. *E.g., Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *see generally* Ian C. Ballon, "eCommerce and Internet Law: Legal Treatise with Forms 2d ed." Section 27.07 (West 2008 & 2019 Cum. Supp.).

Standing is important in cybersecurity cases because the typical plaintiff has not experienced any financial loss as a result of the breach which forms the basis for the lawsuit.

By 2019, almost all Americans have had their information compromised at one time or another — and typically multiple times. While almost everyone who has used the internet has, at some point, had their personal information exposed to hackers, only a small percentage have been victims of identity theft or otherwise experienced financial loss from a breach.

The typical cybersecurity class action involves the allegation that a large number of people had their information compromised, even though they suffered no financial harm or identity theft as a consequence of the alleged breach. For this reason, plaintiffs' counsel typically prefer to be in federal court — on the theory that a larger potential class of people who have no out of pocket losses will have greater settlement value than a class of similarly situated people in a single state.

While cybersecurity cases may suffer from multiple defects from a defense perspective — including causation (because a breach may expose information that previously was exposed in another breach or which can't be used for identity theft or to cause financial harm) — standing frequently is a threshold obstacle for plaintiffs to get past in cases based on the threat of future harm, where named plaintiffs have not incurred any financial loss.

The U.S. Supreme Court, in *Clapper v. Amnesty International USA*, held that to establish Article III standing a plaintiff must allege an injury that is concrete, particularized and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling. *Clapper* made clear that, to establish standing, a future injury must be "certainly impending," rather than speculative or based on "a highly attenuated chain of possibilities." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409-11 (2013).

Clapper means that in most cases a breach that has exposed someone's

Take steps to mitigate exposure to privacy litigation

information but has not resulted in any actual financial loss cannot form the basis for standing. Nor can remediation efforts to address a speculative harm form the basis for standing. As the Supreme Court explained in *Clapper*, plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 402, 407. The Supreme Court explained that allowing plaintiffs to bring suit "based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of [their] first failed theory of standing." *Id.* at 416.

The 6th and 7th Circuits, however, have held that a company's decision to offer credit monitoring to customers following a security breach evidenced that the risk of harm was more than de minimis and therefore plaintiffs provided with credit monitoring services had Article III standing to sue over the security breach. *See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015); *see also Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (adopting the same analysis in an unreported, 2-1 decision). In a subsequent 7th Circuit case, the court even found standing where the plaintiff had purchased credit monitoring services well before the breach but alleged that his decision to renew those services was largely based on the defendant's security breach. *See Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827-30 (7th Cir. 2018) (holding that one of the two plaintiffs had stated a claim for damages because the plaintiff had standing to assert Illinois state law claims against a merchant for a security breach arising out of compromised PIN pads used to verify credit card information, where the plaintiff alleged that (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her card for several days, and (2) the security breach at Barnes & Noble "was a decisive factor" when she renewed a credit-monitoring service for $16.99 per month); Ballon, Section 27.07.

By contrast, the 4th Circuit rejected this approach, as inconsistent with *Clapper*. It explained that, "[c]ontrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals. To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit." *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir.), *cert denied*, 137 S. Ct. 2307 (2017).

Nevertheless, just last year the 9th Circuit, consistent with the more permissive view of Article III jurisdiction, cited a routine, boilerplate warning that users should change their passwords, following a security breach, as evidence of the severity of the breach, which supported the finding of standing in that case. *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-30 (9th Cir. 2018).

While the 6th, 7th, 8th and D.C. Circuits have set a lower bar for what satisfies the requirements for Article III standing in a cybersecurity case — characterizing as a present injury, for example, the time and expense incurred contacting credit card companies or otherwise mitigating the risk of future harm — the 2nd, 3rd, 4th and 8th Circuits have issued opinions in cybersecurity cases that set a higher threshold to establish injury, consistent with *Clapper*. *Compare Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016) (2-1; unreported); *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015); *Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963 (7th Cir. 2016); *Dieffenback v. Barnes & Noble, Inc.*, 827 F.3d 826 (7th Cir. 2018); *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); *with Whalen v. Michael's Stores, Inc.*, 689 F. App'x. 89 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763 (8th Cir. 2017); *see also Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012) (pre-*Clapper* case consistent with *Clapper* in finding no standing in a cybersecurity breach case); *see generally* Ballon, Section 27.07.

For example, the 4th Circuit rejected the argument that data breaches create an enhanced risk of future identity theft, as too speculative, in the face of evidence presented that 33 percent of health related data breaches result in identity theft. Similarly, the 8th Circuit affirmed dismissal for lack of standing of the claims of 15 of the 16 plaintiffs who had not incurred financial harm, but held that the one plaintiff who alleged he suffered a fraudulent charge on his credit card had standing to sue.

By contrast, the 9th Circuit cited the fact that others, not before the court, had experienced financial loss allegedly from the same security breach, as evidence of standing for a putative class of those who had not experienced loss, which amounts to a bootstrapping argument that directly contradicts the Supreme Court's analysis in *Clapper*. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-30 (9th Cir. 2018); Ballon, Section 27.07.

This circuit split means that, in some cases, where a company is sued can be outcome determinative on the issue of standing.

While companies may be able to address this problem through venue selection clauses (*see, e.g., Atlantic Marine Construction Co. v. U.S. District Court for the Western District of Texas*, 571 U.S. 49, 62-63 (2013); Ballon, Section 54.02), and the U.S. Supreme Court may well resolve the current split in a future case, the most effective way for businesses to address the uncertainty associated with conflicting standards in litigation is through enforceable arbitration provisions, with a binding delegation clause. *See, e.g., Henry Schein, Inc. v. Arhcer & White Sales, Inc.*, 2019 DJDAR 147 (U.S. Jan. 8, 2019); *Rent-A-Center, West, Inc. v. Jackson*, 130 S. Ct. 2772 (2010); *see generally* Ballon, Section 22.05[2][M].

In light of a different circuit split, the arbitration clause also should include an express class action waiver (*see Spirit Airlines, Inc. v. Maizes*, 899 F.3d 1230 (11th Cir. 2018) (disagreeing with four other circuits in holding that incorporation by reference of AAA rules delegates the issue of whether arbitration may proceed on a class-wide basis to the arbitrator, not the court, if the contract is otherwise silent about whether it provides for individual or class arbitration)), even though the U.S. Supreme Court has held that consent to class arbitration must be express, and cannot be inferred from silence. *See Stolt-Nielsen S.A. v. AnimalFeeds Int'l Corp.*, 559 U.S. 662 (2010).

With the volume of cybersecurity litigation likely to increase in California once the California Consumer Privacy Act (Cal. Civ. Code Sections 1798.100 to 1798.199) and California's Internet of Things (IoT) security law (Cal. Civil Code Sections 1798.91.04 to 1798.91.06) take effect on Jan. 1, 2020, California businesses need to take proactive steps to mitigate their risk of exposure to cybersecurity breach litigation, including by entering into binding arbitration agreements with users. Given the cost of litigation, business entities should review the enforceability of their consumer contracts, including especially online and mobile Terms of Service and Privacy Policies, on a regular basis to account for shifting legal doctrines and circuit splits on key issues.

Ian Ballon *has served as lead counsel in successfully defending numerous cybersecurity breach and data privacy class action suits. He is co-chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and a litigation shareholder in the firm's Silicon Valley and Los Angeles offices. He is also the author of West's 5-volume treatise, E-Commerce and Internet Law 2d edition (www.ianballon.net), which he updates annually "in his spare time." He may be reached at Ballon@GTLAW.com.*

BALLON