Issue No. 1 in Anthem data breach class actions: does the Supreme Court's ruling in Clapper prevent standing?

February 20, 2015

As of this writing, class actions have been filed against Anthem in the federal courts of the Southern District of Ohio, Northern District of Ohio, Northern District of Alabama, Northern District of Georgia, Southern District of Indiana and Central District of California. There will be more. The speculative nature of harm in data breach cases means that Article III standing will be hotly contested in each. In this article, we review the legal landscape of this fundamental requirement for federal jurisdiction.

Background on Article III Standing in Data Breach Cases

As we previously discussed, Article III of the U.S. Constitution continues to grab headlines in class action litigation as one of the most potent barriers to class certification. With increasing frequency, courts are asking whether class representatives — and the class members they seek to represent — have suffered injuries that are sufficient to satisfy the most fundamental test of Article III standing. Class plaintiffs are being tossed out of court with ever increasing frequency because their damage claims are simply too tenuous to pass constitutional muster.

In the data breach area in particular, we have noted that plaintiffs have historically struggled to establish Article III standing for common law negligence or invasion of privacy claims, because an actual injury in fact is often unsubstantiated. Data breach plaintiffs have been successful when they have provided factual support for a credible threat of immediate harm. Another popular strategy for class plaintiffs is to bring data breach claims under one or more of various federal and state statutes related to privacy or consumer protection. For example, the Telephone Consumer Protection Act (TCPA) provides a private right of action and statutory damages. Other similar consumer protection statues also provide for the recovery of attorney's fees. However, the strategy of framing one's case as a statutory violation brings with it the additional burden of having to meet the often highly technical requirements of the chosen statute(s).

Of course, some statutory and regulatory requirements related to data security expressly foreclose a private right of action for violations. For example, the Health Insurance Portability and Accountability Act (HIPAA) expressly precludes a private right of action and preempts state and local laws and regulations unless they are more stringent than HIPAA. For this reason, plaintiffs, such as those suing Anthem, attempt to frame an alleged HIPAA violation in terms of a breach of contract, undue enrichment, bailment, negligence or a privacy-related tort.

Regardless of the how the claims are framed, to pass constitutional muster under Article III, plaintiffs must demonstrate three elements. The "injury must be [1] concrete, particularized, and actual or imminent; [2] fairly traceable to the challenged action; and [3] redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013). "The party invoking federal jurisdiction bears the burden of establishing these [standing] elements." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). In a class action, the class representatives "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 and which they purport to represent." *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976).

Along Comes *Clapper*

In *Clapper v. Amnesty Int'l USA*, respondents challenged the Foreign Intelligence Surveillance Act of 1978, which permitted surveillance of individuals who were not "'United States persons' and [were] reasonably believed to be located outside the United States." *See Clapper*, 133 S. Ct. at 1142. The respondents were various persons who argued that they would likely engage in sensitive communications with individuals who would be targets of surveillance under the act. In this context, the Supreme Court provides substantial guidance on the more generally applicable standard for establishing injury in fact. That is, how far does "actual or imminent" really extend?

While conceding that "imminence" is "a somewhat elastic concept," the Court notes that this term "cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes — that the injury is *certainly* impending." *Id.* at 1147. As such, the Supreme Court goes on to note: "we have repeatedly reiterated that 'threatened injury must be *certainly* impending to constitute injury in fact,' and that '[a]llegations of possible future injury' are not sufficient." *Id.* In applying this precedent, the Court in *Clapper* expressly rejected the Second Circuit's "objectively reasonable likelihood" standard. *Id.*

Clapper also speaks to another general standing issue highly relevant in data breach cases: where independent third parties are involved, such as hackers in the context of a data breach case, will they act in such a manner as to bring about actual harm to a plaintiff?

The issue in *Clapper*: "even if respondents could demonstrate that the targeting of their foreign contacts is imminent, respondents can only speculate as to whether the Government will seek to use §1881a-authorized surveillance (rather than other methods) to do so." *Id.* at 1149–50. In reviewing its precedent on this point, the Court notes: "we have been reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment." As such the Court declines to abandon its "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors." *Id.* at 1150.

Clapper tempers its analysis by acknowledging that Supreme Court precedent does "not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about." *Id.* at 1150, n.5. Standing has been found based upon a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm. *Id.* While withholding comment on whether the "substantial risk" standard is relevant and distinct from the "clearly impending" requirement, the Court holds that, to the extent there is any relevant difference, respondents in this case have not demonstrated "substantial risk" because of the "attenuated chain of inferences necessary to find harm here." *Id.*

Data Breach Class Action Standing in the Wake of *Clapper*: Still Split

Following *Clapper*, the majority of courts facing a data breach class action have applied the Supreme Court's precedent in dismissing claims for lack of standing where personal information is stolen, but no actual identity theft is alleged. That said, the cases are not uniform and some have begun to point to the Supreme Court's more recent decision on Article III standing, *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (2014), to infer a less rigorous standard.

A Sampling of Majority View Cases

Southern District of Ohio: *Galaria v. Nationwide*

The Southern District of Ohio's decision in *Galaria v. Nationwide* is representative of majority view cases. Here, the court has little difficulty in applying *Clapper* to dismiss the plaintiffs' Fair Credit Reporting Act (FCRA), negligence, invasion of privacy and bailment claims. *See Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio Feb. 10, 2014). In fact, the *Galaria* court actually took the issue up on its own after the defendant insurance carrier conceded statutory standing with respect to the plaintiffs' claim for willful violation of FCRA. *Id.* at 552.

The facts of *Galaria* read like those of many data breach cases in the news recently. The defendant insurance carrier informed its insureds that thieves had hacked its computer network and, as a result, personally identifying information (PII) was stolen and disseminated. Id. at 650. The defendant offered one year of free credit monitoring and identity theft protection and suggested to

its insureds that they place a security freeze on their credit reports at their own expense. *Id*. The plaintiffs' claim of damages can be grouped into three broad categories: (i) increased risk of harm/cost to mitigate increased risk; (ii) loss of privacy; and (iii) deprivation of the value of PII. *Id*.

The *Galaria* decision provides a lengthy review of case law from around the country on the question of whether increased risk is sufficient to establish standing. The court comes down firmly in the anti-standing camp, noting that the pro-standing cases it reviewed were all decided prior to *Clapper*. *Id*. at 654–56. Noting *Clapper* expressly rejected the Second Circuit's more lenient "objectively reasonable likelihood" test, the *Galaria* court reasons that logically, *Clapper*'s precedent would also overrule what the court describes as the Ninth Circuit's even lower "not merely speculative" test. *Id*.

On the facts before it, *Galaria* finds that allegations of a 19 percent incidence of fraud "can hardly be said to be 'certainly impending'" injury. *Id*. at 654. Nor, for that matter, do they represent a "substantial risk," using the Supreme Court's alternative terminology. *Id*. at 654 n.8. And, since any harm would depend upon what the third party criminals might do with the information they stole, per *Clapper*, any harm stemming from the stolen data is merely speculative anyway. *Id*. at 655.

Therefore, given the speculative nature of alleged harm, the plaintiffs' allegations of injury based upon their out-of-pocket costs for the increased risk of identity theft, identity fraud, medical fraud and phishing are likewise speculative. Quoting *Clapper* again, the court notes: "Such injury does not suffice to confer standing because 'respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'" *Id*. at 657.

With respect to the plaintiffs' allegations of harm based on loss of privacy, the *Galaria* court agrees that such loss is not speculative, but notes that this does not end the inquiry. For standing, plaintiffs must further show that the harm is "concrete and particularized." *Id*. at 658. Here, the court draws a distinction between common law negligence and bailment claims on one hand, for which plaintiffs lack standing, and their claim brought under the Ohio recognized tort of invasion of privacy, on the other hand, for which the court finds standing. *Id*. at 658.

Although finding standing on the invasion of privacy claim, the court ultimately grants the defendant's motion to dismiss this claim with prejudice because the allegations fail to sufficiently allege the elements of the claim. The court reasons that merely alleging that criminals stole plaintiffs' information from the defendant does not demonstrate the required element of "dissemination" by the defendant. And, even assuming dissemination, the complaint fails to allege the required element of "publicity" because even if the hackers have the information, there is no allegation that the information has become public knowledge. *Id*. at 661–62.

Lastly, the *Galaria* court rejects standing for the plaintiffs' third category of alleged injury: "Regardless of whether Named Plaintiffs argue the value of their PII has merely diminished or whether they allege complete deprivation of value, they have failed to allege any facts explaining how their PII became less valuable to them (or lost all value) by the data breach." *Id*. at 660. In other words, unless the plaintiffs can show how they could and would have monetized the value of their PII if not for the breach, there is no injury. *Id*.

District of Columbia: *SAIC Backup Tape Data Theft Litig.*

The District of Columbia similarly views *Clapper* as clarifying that alleging "increased risk," alone, is insufficient to confer standing for a data breach class action case. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 2360, 2014 U.S. Dist. LEXIS 64125, R *32 (D.D.C. May 9, 2014) ("Indeed, since *Clapper* was handed down last year, courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases.").

Likewise, an allegation that data was stolen, without more, does not confer standing for invasion of privacy. In this case, "the information itself is locked inside tapes that require some expertise to open and decipher. Indeed, it is highly unlikely that the crook even understood what the tapes were, let alone had the wherewithal to access them or navigate her way to any one of the 4.7 million records contained therein." *Id*. at *35. Therefore, the few plaintiffs who do allege that their data was used have standing while the rest "are out of luck." *Id*. at *36.

The court declines to presume that the remaining plaintiffs' information will suffer the same fate as the two plaintiffs allowed to go forward, reasoning:

> Here, only six Plaintiffs allege some form of identity theft, and out of those six only Curtis offers any plausible link to the tapes. And Yarde is the only other Plaintiff — out of a population of 4.7 million — who has offered any evidence that someone may have accessed her medical or personal information.
>
> Given those numbers, it would be entirely implausible to assume that a massive identity-theft scheme is currently in progress or is certainly impending. Indeed, given that thirty-four months have elapsed, either the malefactors are extraordinarily patient or no mining of the tapes has occurred. This is simply not a case where hundreds or thousands of instances of fraud have been linked to the data breach. Rather, as far as the Court is aware, only six instances of fraud have been reported, and only two customers can plausibly link either identity theft or privacy violations to the tapes' loss. As such, only those two Plaintiffs whose harm is plausibly linked to the breach may move forward with their claims.

Id. at *48-51.

Northern District of Illinois: *Strautins and In re Barnes & Noble Pin Pad*

Like the cases above, in *Strautins*, the Northern District of Illinois does not hesitate to recognize that "*Clapper* compels rejection of [plaintiffs'] claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing." *See Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014). In *Strautins*, the district court noted that *Clapper* controls on this issue and, therefore, the court is obligated to disregard the "seemingly inconsistent Seventh Circuit precedent that predates *Clapper*," notably, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007). *See Strautins*, 27 F. Supp. 3d at 879.

In an earlier case, *In re Barnes & Noble Pin Pad*, the Northern District of Illinois likewise applied *Clapper* to dismiss all of the plaintiffs' claims for lack of standing. *See* 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sept. 3, 2013). Though the plaintiffs failed to allege imminent harm in this case, it was not for a lack of creative thought on all the different ways to describe their injury. The alleged injury to the named plaintiffs in *Barnes & Noble* includes: "untimely and inadequate notification of the security breach, improper disclosure of Plaintiffs' PII, invasion of privacy, expenses incurred in efforts to mitigate the increased risk of identity theft or fraud caused by the security breach, time lost mitigating the increased risk of identity theft or fraud caused by the security breach, an increased risk of identity theft, deprivation of the value of Plaintiffs' PII, anxiety and emotional distress, and diminished value of products and services." *Id.* at *8.

Questioning *Clapper*'s Applicability in Data Breach Class Actions

Northern District of Illinois: *Moyer v. Michaels Stores, Inc.*

In *Moyer*, Judge Bucklo departs from her Northern District of Illinois colleagues by questioning the applicability of *Clapper* and choosing to instead follow the earlier Seventh Circuit precedent in the *Pisciotta* case. *See Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *15 (N.D. Ill. July 14, 2014).

In finding standing under what the court views as a less rigorous standard in *Pisciotta*, the court begins by distinguishing *Clapper*: "[t]he extent to which *Clapper*'s admittedly rigorous standing analysis should apply in a case that presents neither national security nor constitutional issues is an open question." *Id*. at *15 (noting that *Strautins* described this point as one in which reasonable minds may differ).

Next, *Moyer* notes that the Supreme Court's most recent decision on the injury-in-fact requirement, *Susan B. Anthony List*, catalogues the myriad circumstances in which a risk of future harm — such as enforcement of an allegedly unconstitutional law — has been deemed sufficiently imminent to establish Article III standing. The court further notes that the labels used to describe the imminence requirement in these cases cataloged by the Supreme Court — i.e., injury risks that are not "chimerical," "imaginary" or "wholly speculative," or, conversely, ones that are "credible" and "well-founded" — sound less demanding than *Clapper*'s rigorous application of the "certainly impending" standard. *Id.* at *15-16 (citing *Susan B. Anthony List*, 133 S.Ct. at 1147).

The *Moyer* court proceeds to reason that "Although Plaintiffs cannot establish standing based solely on [one of the named plaintiffs'] injuries, the fraudulent charges she incurred within two weeks of shopping at Michaels informs my analysis of whether the risk of identity theft facing these Plaintiffs is substantial and well-founded. [...] The allegation that [one of the named plaintiffs] incurred fraudulent credit card charges makes this case analogous to cases where the Court found a sufficiently imminent risk of injury based on evidence that the relevant risk had materialized in similar circumstances." *Id.* at *17. In other words, the *Moyer* court was willing to consider the very kind of speculation that the District Court of Columbia refused to engage in the *SAIC* case.

Finally, the *Moyer* court finds that "the chain of causation connecting a data security breach and identity theft is not so attenuated that is makes the latter risk speculative or hypothetical." *Id.* at *17-18. Applying another Supreme Court ruling in a non-data breach case to the current situation, the *Moyer* court reasons:

> If a bee's anticipated pollination patterns create a sufficiently imminent risk of injury to alfalfa farmers who fear gene flow from genetically engineered plants in nearby fields, I fail to see how the transfer of information from a data hacker to an identity thief (assuming they are not one and the same) could be deemed an overly attenuated risk of harm.

Id. at *19 (citing *Monsanto v. Geertson Seed Farms*, 561 U.S. 139 (2010)).

Though finding standing, the court ultimately granted the defendant's motion to dismiss, because the plaintiffs failed to allege all necessary elements of their underlying claims. *Id.* at *24.

Southern and Northern District of California: *Sony Gaming and Adobe Systems*

As noted above, the Supreme Court's decision in *Clapper* expressly rejects the Second Circuit's "objectively reasonable likelihood." While *Clapper* did not have before it and, therefore, does not opine on the Ninth Circuit's formulation of the imminence standard, some lower decisions outside of the Ninth Circuit have suggested that *Clapper* similarly modifies the precedent in the Ninth Circuit. *See Galaria*, 998 F. Supp. 2d 646 (S.D. Ohio Feb. 10, 2014). The Southern and Northern Districts of California have each issued decisions flatly rejecting this view.

In the case of *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014), the court reasons:

> [A]lthough the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be "certainly impending," rather than "real and immediate," the Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be "real and immediate." To the contrary, the Supreme Court's decision in *Clapper* simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an "injury-in-fact" for

> purposes of establishing Article III standing.

Id. at 961. Therefore, the court finds both *Clapper* and *Krottner* controlling, and case law in the Ninth Circuit analyzing the "injury-in-fact" requirement following *Krottner* highly persuasive. *Id.*

Under this dual standard, the court finds that the plaintiffs' allegations, which fail to include any allegation that information was actually accessed by a third party, are sufficient to confer standing. In the *Sony Gaming* court's view, neither *Krottner* nor *Clapper* require such allegations. The breach alone is sufficient to show "a 'credible threat' of impending harm based on the disclosure of their Personal Information following the intrusion." *Id.* at 963.

In *Adobe Systems*, the Northern District of California follows essentially the same analysis as *Sony Gaming* in finding that *Krottner* remains controlling precedent following *Clapper*. *See In re Adobe Sys. Privacy Litig.*, No.: 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal. Sept. 4, 2014). Also like *Sony Gaming*, the court in *Adobe Systems* finds the plaintiffs' allegations sufficient under its reading of both standards. Here, the court states "there is no need to speculate" whether information was stolen or "whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so." *Id.* at *27-29 (noting in particular: "Some of the stolen data has already surfaced on the Internet, and other hackers have allegedly misused it to discover vulnerabilities in Adobe's products.").

Adobe Systems also rejects the necessity for plaintiffs to "allege that their stolen personal information had already been misused," reasoning that "to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact." *Id.* at *28.

So Is There Standing in Anthem?

The answer is one only a lawyer could love: "it depends." More particularly, it apparently depends a lot on where the case is brought.

Looking solely at the standard for "imminence" in each jurisdiction, and setting aside the allegations in each complaint, it appears that the cases in Ohio, Alabama and Georgia will face the most difficult hurdles for standing. *See Galaria v. Nationwide* discussed above and *Eternal Word TV Network, Inc. v. Sebelius*, 935 F. Supp. 2d 1196 (N.D. Ala. 2013) ("[A] recent United States Supreme Court case [*Clapper*], reiterates a point that the Court has repeatedly made regarding standing: namely, that 'allegations of possible future injury' are not sufficient to confer standing."); *Locklear v. Dow Jones & Co.*, No. 1:14-CV-00744-MHC, 2015 U.S. Dist. LEXIS 16301, at *5-6 (N.D. Ga. Jan. 23, 2015) (also following *Clapper*).

The case in California appears to have the most favorable case law for standing in view of *In re Sony Gaming* and *Adobe Systems*.

Meanwhile, the conflicting views of the Northern District of Illinois in *Strautins*, *Barnes & Noble* and *Moyer* will create some interesting persuasive authority within the Seventh Circuit for the Southern District of Indiana to ponder in that case. While the Southern District of Indiana does not appear to have yet addressed standing in a data breach case following *Clapper*, in a recent non-data breach case, the Southern District of Indiana does apply the standard from *Susan B. Anthony List*, which, as noted above, the *Moyer* court suggests is less rigorous than *Clapper*. *See Indiana v. IRS*, No. 1:13-cv-1612-WTL-TAB, 2014 U.S. Dist. LEXIS 111068, at *12-13 (S.D. Ind. Aug. 12, 2014).

Authors