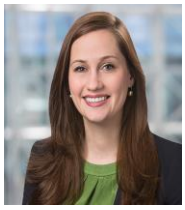
Standing in the Midst of a Data Breach Class Action

By: Allison Holt, Joby Ryan and Joseph W. Ryan, Jr.



Allison Holt is a Senior Associate in the D.C. office of Hogan Lovells. Her practice focuses on cyber security and data breach litigation, where she counsels clients on all manner of matters, including coordinating incident response and forensic investigations, advising on regulatory investigations, and representing clients in complex and multijurisdictional litigation. Prior to joining Hogan Lovells, Ms. Holt clerked for the Honorable Gilbert Merritt of the U.S. Court of Appeals for the Sixth Circuit. She is a graduate of Vanderbilt Law School and Lipscomb University.

Joby Ryan is a Development Officer with the University of Virginia Law School Foundation. He joined the Law School in 2013 as the Director of the Career Services Office after practicing at Hogan Lovells in D.C. for nearly eight years. Mr. Ryan's practice at Hogan Lovells focused on securities litigation and antitrust. He is a graduate of the University of Virginia Law School and Harvard College.

Joe Ryan is a trial lawyer who focuses his practice in the area of complex professional liability, intellectual property, class actions, and commercial law. Mr. Ryan represents corporate clients throughout the country on trademark, service mark, and trade dress claims. In 2010, Mr. Ryan served as President of the IADC.

IT'S among an in-house lawyer's greatest nightmares: a call from an employee in the company's information security department reporting anomalous and unauthorized activity in the company's databases. Over the next few days, the reality of the situation unspools quickly—often with inadvertent misinformation at several points along the way. The company has been attacked. Personally identifiable data of its customers or employees has been accessed and possibly exfiltrated by criminals.

Critical decisions must be made immediately, and those initial decisions may have severe implications for inevitable future class action lawsuits brought in response to the data breach or cyberattack. Should the company bring in outside forensic assistance? If so, which outside forensic firm offers the most credibility for the investigation? Should the company offer credit monitoring services? For how long? Through which provider? What mandated notice is required to regulators and affected individuals? How can the company minimize the P.R. damage? The list goes on and on.

Unfortunately, the scene above is playing out more and more frequently. Criminal cyberattacks are a very real danger for corporations (and even law firms). As a result, corporate counsel must grapple with an emerging new area of potential exposure for suits brought by individuals whose personal or financial data may have been affected.

A company's response in the immediate aftermath of a cyberattack or data breach, press releases, forensic investigations, notices to customers, offers of credit monitoring, and all the rest, is merely prelude. No matter how prompt and thorough a corporate victim's response to a data breach is, a breach of any discernible size will inevitably bring large-scale litigation. These cases nearly always take the form of a class action, where a handful of named plaintiffs seek to represent the interests of a purported class of alleged affected individuals seeking recovery for their personal or financial data potentially being compromised as a result of the breach.

As a threshold question, one might reasonably ask whether a cause of action even exists, given that the defendant corporations are, in nearly all cases, victims of a crime themselves. Indeed, in some cases, these cyberattacks are not merely crimes but acts of foreign espionage or foreign military conduct.[1] Data breach cases thus create a

[1] Consider the OPM cyberattack (allegedly conducted by Chinese militants), the Sony hack (allegedly North Korea) and the breach

conundrum where a company is both a victim and a defendant called to account in court for its victim status. Even so, corporations continue to face significant litigation following a cyberattack. Corporate counsel's first best chance to dispose of these cases is often by challenging plaintiffs' standing.

This article will thus focus primarily on Article III standing. There are numerous issues at play in data breach cases (discovery disputes, class certification, etc.), but the fight over standing is particularly salient because i) the landscape continues to mature and ii) a court's ruling on standing determines whether a case can proceed to the costly discovery and class certification stages. Moreover, despite nearly 15 of years of litigating this issue and two applicable Supreme Court rulings, the terrain remains uncertain.

I. Plaintiffs' Most Common Allegation in Support of Standing in Data Breach Litigation Is Heightened Risk of Future Harm

When purported data breach class action cases are filed in federal court the first battleground is likely to be whether the plaintiff class has standing to sue under Article III. Because the federal court system is one of limited jurisdiction, in order to sue in federal court Article III requires that plaintiffs have standing to be there. The constitutional minimum for standing contains three elements: a plaintiff must have suffered an injury-in-fact, the injury must be causally connected to the challenged action of the defendant, and the injury must be redressable by a favorable decision.[2] The law is clear that allegations of possible future injury will not satisfy the standing requirement. Rather, plaintiffs must allege injury that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[3]

A. Risk of Future Harm: The Early Years

Historically, Article III's injury-in-fact requirement has been the biggest obstacle to plaintiffs' pursuit of class action litigation in the wake of a data breach. The most common theory of harm on which plaintiffs attempt to support such cases is the allegation that they suffer an increased risk of future identity theft or fraudulent charges by virtue of their personally identifying information ("PII") being com-promised. Most early courts to face this issue held that plaintiffs' alleged

---

of the Democratic National Committee's email server (allegedly Russia) to name a few high-profile examples.

[2] *See* Lujan v. Defs. Of Wildlife, 504 U.S. 555, 560-561 (1992).

[3] *Id*.

increased "risk of future harm" was not sufficient to support standing.[4]

In *Reilly v. Ceridian*, for instance, plaintiffs brought a putative class action against a payroll processing firm when an attacker infiltrated its system and potentially gained access to financial information for 27,000 employees at 1,900 companies. On appeal, the Third Circuit upheld the District Court's dismissal for lack of standing, explaining that the alleged increased risk of injury did not constitute actual injury because:

> [W]e cannot describe how the Appellants will be injured in this case without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury.... The present test is actuality, not hypothetical speculations concerning the possibility of future injury.[5]

But not all circuits followed this early trend. In 2007, the Seventh Circuit found standing in *Pisciotta v. Old National Bancorp.*, in which plaintiffs brought a class action against a bank after its website had been breached, alleging that the bank failed to adequately secure the personal information (including PII) it solicited on its website.[6] Plaintiffs' rested their theory of injury entirely on increased risk that their personal data would be misused in the future; they did not allege "any completed *direct* financial loss to their accounts" nor that they "*already had been* the victim of identity theft as a result of the breach."[7] In finding standing, the court surveyed cases in toxic substance, medical monitoring and environmental tort contexts, and concluded, "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[8]

The Ninth Circuit made a similar finding a few years later in *Krottner*

---

[4] *See, e.g.*, Reilly v. Ceridian Corporation, 664 F.3d 38, 43 (3rd Cir. 2011) ("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 a person whose information *may* have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative.").

[5] *Id*. at 43 (emphasis in original).

[6] 499 F.3d 629 (7th Cir. 2007).

[7] *Id*. at 632.

[8] *Id.*

v. Starbucks Corp.[9] In *Krottner*, a laptop containing the names, addresses and social security numbers of 97,000 Starbucks employees was stolen. The court concluded that the plaintiffs had standing to pursue their case because they "alleged a credible threat of real and immediate harm."[10]

1. The Supreme Court Weighs In: *Clapper v. Amnesty International, USA*

Against the backdrop of this circuit split, the Supreme Court decided *Clapper v. Amnesty International, USA*, in which it considered whether risk of future injury satisfies the injury-in-fact requirement for standing under Article III.[11] Clapper is not a data breach case *per se*, but many practitioners speculated that its holding would nonetheless bring clarity to the standing requirements in the data breach context.

Clapper involved a constitutional challenge to government surveillance of suspected terrorists under the Foreign Intelligence Surveillance Act (FISA). Plaintiff-Respondents, who were Americans whose work required them to communicate with the likely subjects of FISA surveillance and thus have their communications surveilled as well, sought a declaratory judgment that provisions of FISA were unconstitutional.[12] The Second Circuit found injury in fact, and thus standing, based on the "objectively reasonable likelihood that [plaintiffs'] communications will be acquired…at some point in the future." The Supreme Court reversed.[13] Writing for the majority, Justice Alito held that "threatened injury must be certainly impending to constitute injury in fact, and allegations of possible future injury are not sufficient."[14] The Court rejected the "objectively reasonable likelihood" standard used by the Second Circuit, finding it "inconsistent with our requirement that threatened injury must be certainly impending to constitute injury in fact."[15]

Despite the seemingly clear mandate that threatened injury must be "certainly impending" to pass Article III muster as injury in fact, *Clapper* included a footnote leaving the door ajar for data breach plaintiffs alleging heightened risk of financial loss or identity theft. The footnote noted that the injury-in-fact requirement does not always require that plaintiffs "demonstrate that [they] are literally certain that

[9] 628 F.3d 1139 (9th Cir. 2010).
[10] *Id*. at 1143.
[11] 133 S.Ct. 1138 (2013).
[12] *Id*. at 1142.
[13] *Id*.
[14] *Id*. at 1147.
[15] *Id*.

the harms they identify will come about. Instead, in some instances, "standing [can be] based on 'substantial risk' that the harm will occur, which may cause plaintiffs to reasonably incur costs to mitigate or avoid the harm."[16] Nevertheless, the import of *Clapper* seemed clear: risk of future injury, if not "certainly impending," would not satisfy plaintiffs' responsibility to plead an injury-in-fact sufficient to confer standing under Article III. And since then, many cases have cited *Clapper* for just that proposition.[17]

2. Post-*Clapper*: Uncertainty Remains as to the Viability of Risk of Future Harm as Grounds for Standing

Practitioners hoping that *Clapper* would usher in an era of clarity in data breach cases regarding whether risk of future injury could satisfy plaintiffs'' Article III standing would soon find themselves disappointed. In two cases after *Clapper*, the Seventh Circuit held the course set out in *Pisciotta*.[18] These cases distinguished *Clapper* to hold that at least in some data breach contexts, a heightened risk of identity theft or fraud can support Article III standing. In *Remijas v. Neiman Marcus*, the Court of Appeals reversed dismissal by the district court finding that plaintiffs whose credit card information was taken as a result of cyberattack of the department store chain had standing to sue. *Remijas* cited *Clapper* for the proposition that "allegations for future harm can establish Article III standing if that harm is "certainly impending," but noted that "*Clapper* does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing."[19] It further distinguished *Clapper* by pointing out that more than 9,000 of the 350,000 impacted credit cards, or about 2.5%, had already shown some attempt at fraudulent charges. From this, the court concluded that the plaintiffs had "no need to speculate as to whether the Neiman Marcus customers' information has been stolen and what information

---

[16] *Id*. at n. 5.

[17] *See e.g.* Khan v. Children's National Health Sys., 88 F. Supp.3d 524, 529 (D. Md. 2016); *In re* Sci. Applications Int'l Corp. (SAIC), 45 F. Supp.3d 14, 24-25 (D. D.C. 2104) ("The degree by which the risk of harm has increased is irrelevant—instead, the question is whether the harm is certainly impending,"); Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) ("we read *Clapper's* rejection of the Second Circuit's attempt to import an 'objectively reasonable likelihood' standard into Article III standing to express the common-sense notion that a threatened event can be 'reasonabl[y] likel[y]' to occur but still be insufficiently 'imminent' to constitute an injury-in-fact,").

[18] Remijas v. Neiman Marcus, 794 F.3d 688 (7th Cir. 2015); Lewert v. P.F. Chang's China Bistro, 819 F.3d 963 (7th Cir. 2016).

[19] *Remijas*, 794 F.3d at 693 (citing n. 5).

was taken." As a result, "the risk that Plaintiffs' personal data will be misused by the hackers…is immediate and very real."[20] After all, the court mused, "why else would hackers break into a store's database and steal consumers' private information? Presumably the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[21]

Therefore, and in light of the fact that some credit cards had already been the subject of fraud, the Court revived the standard that Clapper explicitly rejected. It concluded: "…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.[22]

The Seventh Circuit doubled down on this reasoning in *Lewert v. P.F. Chang's China Bistro*.[23] Again faced with credit card information taken in an attack of defendant's computer system, the court in *Lewer*t relied on *Remijas* to find that "the increased risk of fraudulent charges and identity theft [plaintiffs] face" was sufficiently concrete to support a lawsuit because "their data had already been stolen."[24] The Court found standing because "it is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is 'sooner or later to make fraudulent charges and identity theft.'"[25] In fact, *Lewert* extended *Remijas*: the court also opined that whether the plaintiffs' data was exposed in the breach—something P.F. Chang's disputed—was immaterial to determining standing at the pleading stage.[26] In the Seventh Circuit at least, the risk of future injuries—fraudulent charges and increased risk of identity theft—is enough to support plaintiffs' standing to bring data breach suits.

The Sixth Circuit has followed the Seventh Circuit's lead in *Galaria v. Nationwide Mutual Insurance Co.*[27] The court there found plaintiffs have standing in a case arising out of the theft of their personal information in a breach of Nationwide's

---

[20] *Id*. (citing *In re* Adobe Sys. Inc. Privacy Litig. 66 F. Supp.3d 1197, 1214 (N.D. Cal. 2014)).

[21] *Id*. at 693-694. The *Remijas* Court presumed the intent of the attackers. While the motive behind a cyberattack may seem apparent in cases involving stolen credit card information, inferring intent becomes problematic in other contexts. In some data breach contexts (attacks into massive databases or the misappropriating of other, nonfinancial personal information, for example) the aims of the cyberattackers are more ambiguous or do not relate to the misuse of data. Counsel for corporate defendants should evaluate whether they can draw such distinctions to distinguish the *Remijas* and *Galaria* line of cases.

[22] *Id*. at 693 (citing *Clapper*).

[23] 819 F.3d 963 (7th Cir. 2016).

[24] *Id*. at 967.

[25] *Id*.

[26] *Id*. at 968.

[27] 663 Fed. Appx. 384 (6th Cir. 2016).

computer network because "the theft of their personal data places them at a continuing, increased risk of fraud and identity theft."[28] The court said that unlike *Clapper* and cases like *Ceridian*, where courts needed to speculate future actions to conjure injury, at bar "there was no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."[29]

But not all circuits have read *Clapper* so leniently. Recently, the Fourth Circuit relied on *Clapper* to find that an alleged increased risk of identity theft was too speculative to constitute an injury-in-fact and provide standing under Article III.[30] That consolidated case arose out of the theft of a laptop containing personal information and four boxes of pathology reports containing personal information. The *Beck* court reasoned that the plaintiffs had not claimed either that the thief intentionally targeted their personal information or that there were any instances where any of the stolen data was misused.[31] Plaintiff's sought to rely the Sixth and Seventh Circuit's authority that courts need not speculate about future injury because there was an "identifiable taking" (the laptop and pathology reports had, indeed, been

---

[28] *Id.* at 388.

[29] *Id.* The court in *Galaria* explicitly contrasted its facts with those presented in *Ceridian* because unlike *Ceridian*, it was clear that the cyberattackers took the information. Recall the series of "if's" needed for the plaintiffs to realize injury in *Ceridian*: plaintiffs would only suffer harm "…*if* the hacker read, copied and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully." It is worth noting that only the first of these "if's"—that the attackers had read and copied plaintiffs' data-- was certain in *Galaria*. Whether any particular plaintiff actually experienced any harm still depended on if the attacker understood the accessed information, and if the attacker at some point in the future attempts to use the information and if he does so successfully. Each of these remained open questions in *Galaria*, just as in *Ceridian*, as they do in any data breach case involving plaintiffs who rely solely on allegations of an increased risk of future harm to support standing. Accordingly, other cases have refused to confer standing, even when it is undisputed that the information was taken. *Beck*, 848 F.3d at 276 (finding no standing where information was taken because to do so "we must assume that the thief targeted the stolen items for the personal information they contained… thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This "attenuated chain" cannot confer standing."); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp.2d 1, 7–8 (D. D.C. 2007) (deeming as speculative plaintiffs' allegations "that at some unspecified point in the indefinite future they will be the victims of identity theft" where, although plaintiffs clearly alleged their information was stolen by a burglar, they did "not allege that the burglar who stole the laptop did so in order to access their [i]nformation, or that their [i]nformation ha[d] actually been accessed since the laptop was stolen").

[30] *Beck*, 848 F.3d at 274.

[31] *Id.* at 275.

stolen), but this argument did not persuade the court.

Perhaps unsurprisingly, the lack of uniformity at the Circuit Court level has created divergent outcomes at the District Court level.[32] What practitioners are left with is a true Circuit split, with the Sixth, Seventh and Ninth Circuits holding that increased risk of future harm can suffice as an injury in fact to support standing if the plaintiffs allege an objectively reasonable likelihood that such injury will occur, and decisions from the First, Third and Fourth Circuits that do not,[33] and District Court cases from other Circuits all over the map.[34] As we noted at the outset, the terrain is uneven and uncertain.

3. A New Trend Moving Forward?

A few recent cases have noted a trend amidst all this varying case law. Namely, that in nearly all the cases where standing has been found on allegations of future harm, plaintiffs have set forth "allegations indicating that some of the stolen data had already been misused, that there was a clear intent to use the plaintiffs' personal data for fraudulent purposes, or both."[35] This potential trend has not yet been adopted as a line of demarcation by any Circuit Court beyond the Fourth Circuit, but practitioners should pay attention to this trend line as the case law evolves. With little else to guide defense counsel, particular factors indicating the attackers' intent for the stolen data— particularly evidence of previous fraudulent charges affecting some of the plaintiffs— may well impact whether a court finds the risk of future harm arising from a data breach to be sufficiently imminent and concrete to support standing.

A. Alternative Theories of Injury Alleged to Attempt to Support Standing

Because of the uncertainty surrounding the standing analysis as it pertains to plaintiffs' future risk of harm, many data breach class action plaintiffs now ground their claims of injury in additional types of harm. These typically include costs that plaintiffs expended to mitigate their risk of fraud, overpayment for goods or services

---

[32] *See* Fero v. Excellus Health Plan, Inc., 2017 WL 713660 *8-9 (W.D.N.Y. Feb. 22, 2017) (collecting cases on both sides).

[33] *See In Re* Community Health Systems, Inc. Customer Security Data Breach Litigation, --WL --- (N.D. Ala. February 15, 2017) (Noting split and citing cases).

[34] C*ompare In re SAIC*, 45 F. Supp.3d 14 (D. D.C. 2014) (increased risk of future harm did not support standing after theft of data tapes containing personal information for military members and family) *with In re* Anthem Data Breach Litigation 2016 WL 3029783 at *16 (N.D. Cal. May 26, 2016).

[35] *See Fero*, 2017 WL 713660 at *8-9; *Khan*, 188 F. Supp.3d at 531; *Beck*, 848 F.3d at 274.

(also known as benefit-of-the-bargain), decreased value of their PII, and tethering standing to a statutory violation. For the most part, courts have been more reluctant to ground standing upon these types of allegations, but defense practitioners should be aware of them from the outset of litigation.

1. Mitigation Expenses

In addition to arguing that they suffered a greater risk of future injury arising from the FISA surveillance protocol, plaintiffs in *Clapper* proffered that they were *presently* suffering current injury because they were forced to "take costly and burdensome measures to protect the confidentiality of their international communications."[36] That is, they were forced to take measures to mitigate their heightened risk. Other Plaintiffs have similarly argued that expenses to mitigate risk of identity theft arising from a data breach, including purchasing credit monitoring services and identity theft insurance, constitute present injuries that should confer standing under Article III. The *Clapper* Court rejected this argument, noting that to do otherwise, would "improperly water down" the fundamental requirements of Article III.[37] It would allow plaintiffs to "manufacture standing" by choosing to incur costs in anticipation of non-imminent harm.[38] Most courts have, likewise, refused to allow mitigation expenses such as credit monitoring and identity theft insurance to ground standing.[39]

Rejection of mitigation expenses is not universal, however. Just as it distinguished *Clapper* on the risk of future harm, the Seventh Circuit in *Remijas* distinguished *Clapper*'s instructions regarding mitigating expenses. Noting that it was "important not to overread *Clapper*," the *Remijas* court distinguished the Supreme Court case by stating that "*Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs," whereas the Neiman Marcus customers definitely knew of the increased risk, because Neiman Marcus itself had alerted them to the cyberattack. The future injury was imminent in the court's judgment and mitigation costs were reasonable.[40] It bolstered its reasoning by pointing to the fact that Neiman Marcus had offered free credit monitoring

[36] *Clapper*, 133 S.Ct at 1143.

[37] *Id*. at 1151.

[38] *Id*.

[39] *See, e.g. Beck*, 848 F.3d at 276-277 ("these self-imposed harms cannot confer standing.").

[40] *Remijas*, 894 F.3d at 694.

services to the plaintiffs.[41] More troubling for defense counsel, both *Lewert* and *In Re Anthem* have followed the *Remijas* court's lead. Both cases found that allegations detailing the costs plaintiffs incurred to mitigate risk associated with a data breach were sufficient injuries in fact upon which to ground standing.[42]

2. Overpayment/Benefit of the Bargain

Plaintiffs also argue that they were denied their purported benefit of their bargain with a corporation if their data is exposed as a result of a criminal cyberattack. The theory goes that at least part of the amount paid for a good or service was designated (at least implicitly) for protection of their data.[43] A number of courts have rejected such benefit of the bargain(/overpayment) theory of damages as an injury-in-fact for standing purposes.[44] These allegations sound in breach of contract, unjust enrichment or fraud. The benefit of the bargain allegation is often a heavily fact-driven inquiry, and its success may hinge on particular contractual language or other representations about data security found in service agreements or policy documents. In the health care space, for instance, courts have held at the motion to dismiss phase that plaintiffs have stated claims for breach of contract based on allegations that at least some of their insurance premiums constituted consideration for reasonable data security to be provided by defendant in administering healthcare to plaintiffs.[45] It remains to be seen

---

[41] *Id.* This has implications for both corporate counsel and business leaders. In the wake of a data breach, a corporation must decide whether to provide its customers with free credit monitoring or identity theft protection. Almost all companies choose to provide such monitoring, and the trend is towards more monitoring, not less. Offering customers free credit monitoring can reassure customers that the company is responding appropriately to the breach. But as this excerpt from *Remijas* shows, there are potential downsides to making such an offer. A company's offer to provide credit monitoring services to its customers impacted by a data breach may be viewed as a tacit admission that plaintiffs' fear of a heightened risk of identity theft was reasonable. Corporate counsel should advise business decision makers accordingly.

[42] *Lewert*, 819 F.3d at 967; *In re Anthem*, 2016 WL 3029783 at *16.

[43] An alternative construction is the concept of overpayment: essentially that the plaintiff would not have paid as much for the goods or services had it known that their data would have been susceptible to cyberattack. This is often cast amidst allegations that the defendant company was deficient in protecting the data.

[44] *See Fero*, 2017 WL 713660 at *11 (listing cases).

[45] *See* Resnick v. AvMed Inc., 693 F.3d 1317, 1327-1328 (11th Cir. 2012) (applying Florida law); *In re Anthem*, 2016 WL 3029783 at *13-14; *but see Fero* 2017 WL 713660 at *11 (rejecting standing on overpayment grounds because plaintiffs

whether such theories can survive summary judgment.

3. Decreased Value of PII

Plaintiffs in a data breach class action also argue that their personal information has lost value as a result of its misappropriation and that the purported loss of this value is a present injury that confers standing. Most courts have rejected this theory.[46]

While plaintiffs have an uphill battle to allege that their PII has value, and that it loses part of that value when it is affected in a cyberattack, the argument has been accepted recently by some courts at the motion to dismiss stage.[47] Thus, although it is unlikely such a theory of liability will ultimately prevail, this argument may extend a data breach class action beyond the Motion to Dismiss stage, and propel the case into expensive litigation and class certification stages.

4. Naked Violations of State or Federal Statutes

Another method plaintiffs use in their attempt to plead Article III standing in data breach class actions is alleging violations of various state and federal statutes that arise from the breach. Most courts agree that violations of state statutory law alone cannot establish Article III standing.[48]

It is a more nuanced question when federal statutes are at issue.

"lack[ed] any factual allegations that would support the claim that Plaintiffs paid a specific amount of money for data security."); *Khan*, 188 F. Supp.3d at 533.

[46] *See Fero*, 2017 WL 713660 at *12 ("Courts have rejected allegations that the diminution in value of personal information can support standing"); Welborn v. Internal Revenue Serv., 2016 WL 6495399 *8 (D. D.C. Nov. 2, 2016) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Khan*, 188 F. Supp.3d at 533 (rejecting standing based on diminution in value theory because plaintiff did not "explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information"); Whalen v. Michael Stores, Inc., 153 F. Supp.3d 577, 582 (E.D.N.Y. 2015) ("[W]ithout allegations about how her cancelled credit card information lost value, [plaintiff] does not have standing on this ground."); *In re SAIC*, 45 F. Supp.3d at 30 ("As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss. Even if the service members did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach.").

[47] *See* Claridge v. RockYou, 785 F.Supp.2d 855, 861 (N.D. Cal. 2016) (expressing doubts as to the plaintiffs' theory of damages but allowing discovery); *In re Anthem*, 2016 WL 3029783 at *14-15 ("allegations of diminution in value of her personal information are sufficient to show contract damages [under California law] for pleading purposes.") (Citations omitted).

[48] *Khan*, 188 F.Supp.3d at 534; *Fero*, 2017 WL 713660 (finding that "asserted violations of various state statutes do not confer standing in federal court.").

The Supreme Court has recently addressed the question of whether violation of a federal statute, without more, counts as an injury-in-fact for Article III purposes.[49] It ruled that it does not. In that case, the Court stated that "Article III standing requires a concrete injury even in the context of a statutory violation."[50] For that reason, a plaintiff could not "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[51] *Spokeo* reinforces *Clapper*'s instruction that for Article III standing to lie, plaintiffs' alleged injury must be "concrete," even when alleging a statutory violation. In the context of data breach litigation, *Spokeo* can fairly be read to limit plaintiffs' ability to establish standing in federal courts on a naked statutory violation alone.

Whether *Spokeo* will become an obstacle to class action plaintiffs in data breach cases that do not base their injury upon violation of a federal statute remains to be seen, but post-*Spokeo* cases like *Galaria* and *Fero* suggest that it will not alter the general inquiry laid out in *Clapper*. As with many of the issues in this rapidly evolving area of the law, it remains an open question.

IV. Conclusion

Class-action data breach litigation presents both business and legal challenges with which corporate counsel must grapple from the moment a breach becomes apparent. A corporation's response in the wake of a breach may impact its exposure down the line in litigation. But once suits are filed, the roadmap becomes less clear. Case law is developing quickly and unevenly in this area of law. Issues of standing remain paramount in determining whether these cases survive motions to dismiss, with plaintiffs' success hinging on the court's interpretation of what constitutes an imminent and concrete injury in fact. It's hard to predict how the circuit split will resolve. In light of such uncertainty, corporate counsel should continue to track the trend line noted in *Fero* and *Beck*, that standing may depend on particular factors indicating the attackers' intent for the stolen data. Diligent corporate counsel should also monitor the increasing prevalence and success of allegations of injury beyond increased risk of future harm. If such arguments gain traction with courts, data breach cases could get

[49] Spokeo v. Robins 136 S.Ct. 1540 (2016).
[50] *Id*. at 1549.
[51] *Id.* The Court in *Spokeo* also acknowledged that it did not intend that "the risk of real harm cannot satisfy the requirement of concreteness." This has blunted *Spokeo*'s usefulness to defense counsel as a bar against plaintiffs gaining standing based on allegations of heightened risk of future harm.

even more costly for corporate defendants.