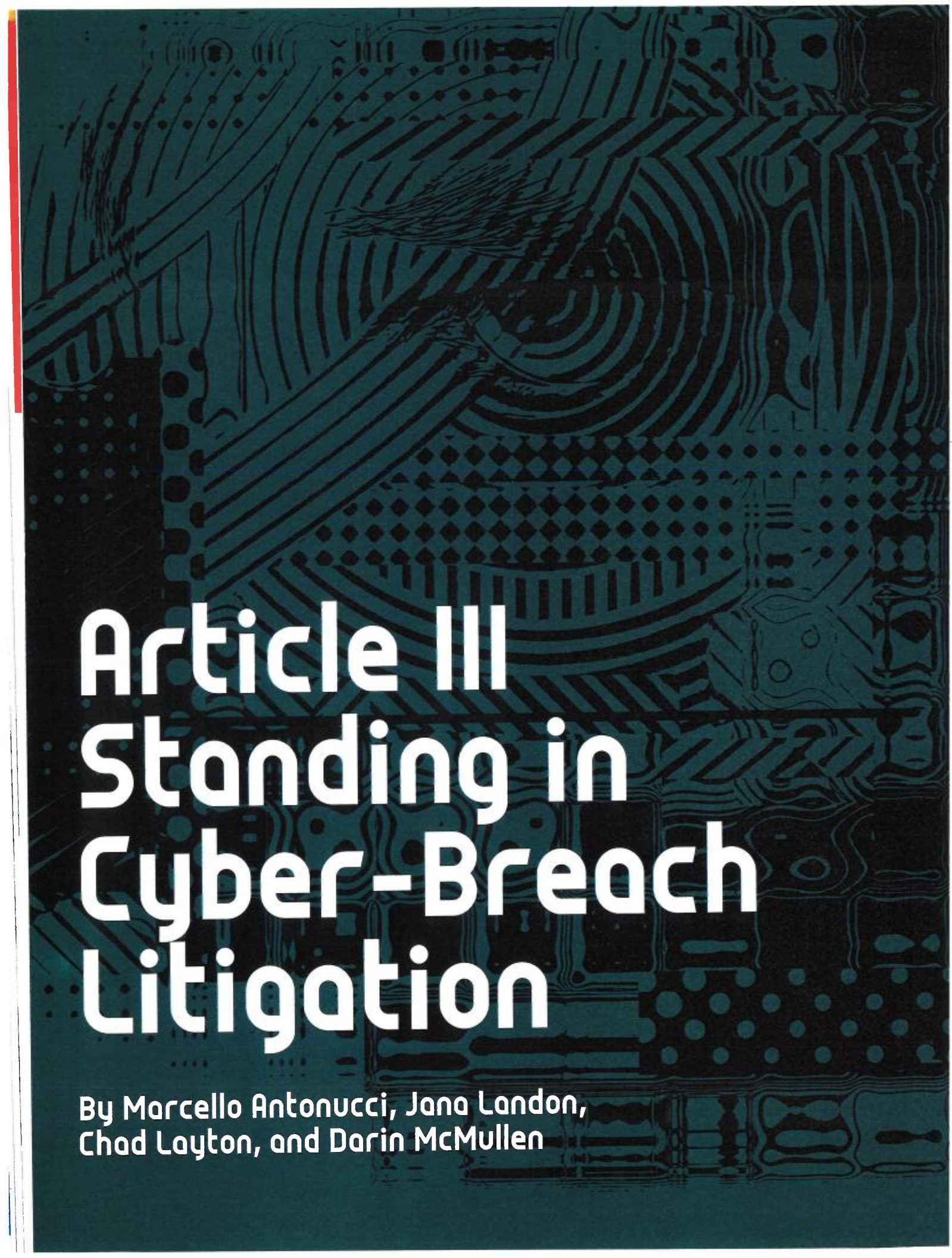
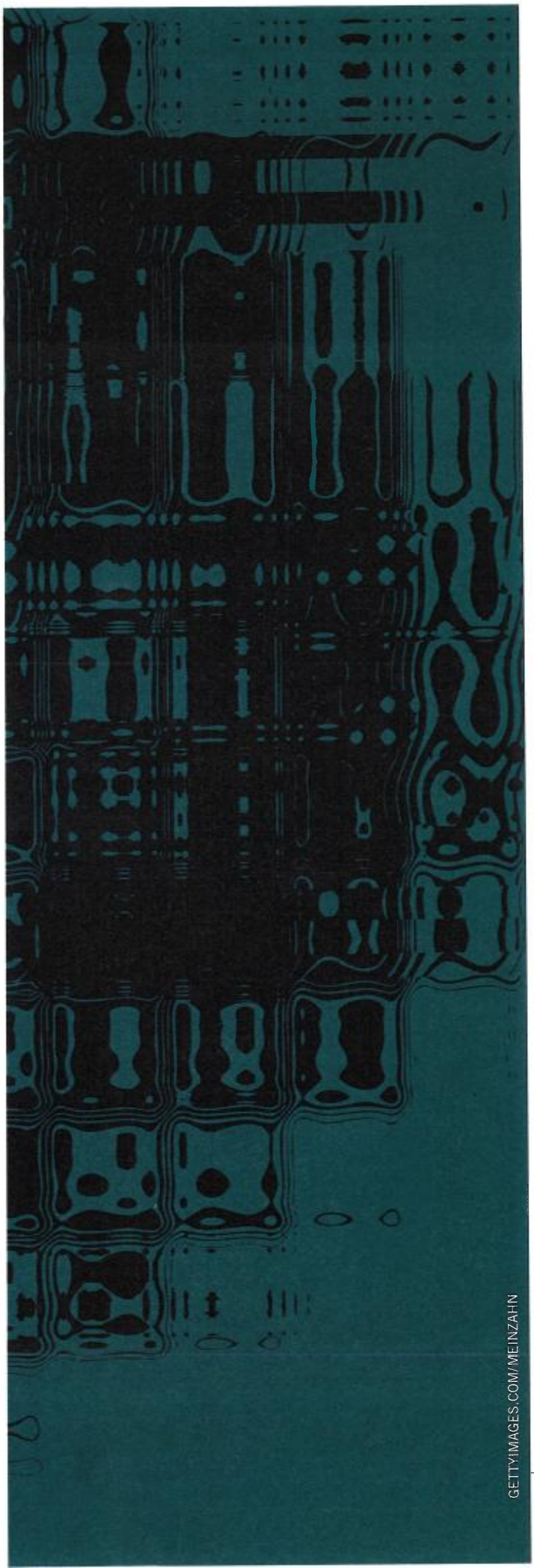


Article III Standing in Cyber-Breach Litigation

By Marcello Antonucci, Jana Landon, Chad Layton, and Darin McMullen



GETTYIMAGES.COM/MEINZAHN

No organization is immune from the risk of a cyberattack. Unfortunately, news of cyberattacks has become commonplace, and such attacks have impacted organizations of all shapes and sizes. It is without question that the risk of a cybersecurity breach is significant, and here to stay. As former FBI director Robert Mueller said while speaking at a cybersecurity conference in 2012, "there are only two companies: those that have been hacked and those that will be."[1] The evidence is compelling that a breach can impact significantly a company in terms of lost reputation, additional costs, and lost business. Not surprisingly, a vast amount of litigation has resulted as a consequence of this risk.

One of the first issues that must be addressed in data breach litigation is whether plaintiffs have legal standing to sue. The concept of standing refers to whether a plaintiff has been injured sufficiently to bring a lawsuit in federal court under Article III of the Constitution. Oftentimes, plaintiffs who are victimized by a data breach may not have suffered any actual or concrete damages. In such cases, a key issue is whether, following a data breach, the increased likelihood of future identity theft, current stress from the breach, or even statutory violations is sufficient to confer standing. The question then becomes whether or not a plaintiff should have the right to pursue a lawsuit where his damages do not constitute an actual economic harm and may be speculative at best.

THE BEGINNING: THE *CLAPPER* AND *SPOKEO* DECISIONS

When determining standing, there are two key U.S. Supreme Court decisions that outline the principles that guide data breach cases filed in federal court. While neither involves data breaches per se, both address damages that were alleged to be speculative. These cases are the fountainhead from which federal-standing jurisprudence in cyber-breach litigation has evolved and will continue to evolve.

***Clapper* and claims of future injury.** The first key decision in this area is *Clapper v. Amnesty International USA*,[2] which involved warrantless wiretapping. The lawsuit was brought by various groups, including reporters who thought that they were being surveilled or might be surveilled. The Supreme Court held that there is no standing for many claims of future injury because such injury is "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[3] Moreover, explained the Court, plaintiffs cannot manufacture standing merely by incurring expenses (for example, by flying to interview sources rather than interviewing them by phone).[4] Although the Court did not rule out standing if the risk of injury was "certainly impending" and there was

TIP

Unlike many other areas of law, the fight over legal standing is more pronounced in cyber-breach litigation, where the existence or absence of Article III standing will make or break a case.

"substantial risk" that harm would occur, the court found that such a burden could not be met by the plaintiffs in this case.[5]

***Spokeo* and particularized injury.** The other key legal decision concerning standing is *Spokeo, Inc. v. Robins*,[6] which held that in order to have standing,

> a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[7]

Furthermore, a plaintiff does not "automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[8]

Spokeo is a company that operates a "people search engine" that aggregates data from various sources. Thomas Robins contended that Spokeo violated the federal Fair Credit Reporting Act (FCRA) when it published false information about him, and he claimed that such information had hurt his job prospects. The Supreme Court found that Robins needed to show (among other things) an "injury in fact" from Spokeo's publication of inaccurate information about him. Moreover, the Court emphasized, the injury needed to be both "concrete and particularized."[9] The Court concluded that Robins had alleged a particularized injury but that a mere procedural violation of the statute was not enough to allege a "concrete" injury.[10] The justices remanded the case to the lower court for further review on the issue of whether Robins had alleged statutory violations that created sufficient risk to meet the concreteness requirement.[11]

CLAPPER AND *SPOKEO*: IMPACT ON DATA BREACH LITIGATION

The legal principles discussed in *Clapper* and *Spokeo* have had a nationwide influence over legal decisions concerning standing in data breach lawsuits.

Standing is a fundamental issue that must exist in every lawsuit. While a dispute concerning the existence of standing is not unique to cyber-related litigation, the issue of standing has become pivotal in such cases, and the nature of the damages—or lack of damages—has brought Article III standing to the forefront of cyber litigation.

Since the Supreme Court's rulings in *Clapper* and *Spokeo*, courts across the country have issued disparate rulings as to what the line should be for conferring standing where actual harm may be nebulous or untraceable to the actual breach event. Several jurisdictions will confer standing despite the absence of an actual economic harm; other courts disagree with this approach. Some jurisdictions have ruled differently in data breach cases and non–data breach cases. In terms of data breach cases, the U.S. Court of Appeals for the Sixth, Ninth, and D.C. Circuits, for example, have recognized that a data breach in and of itself does establish standing;[12] but the First, Second, and Fourth Circuits, for example, have rejected that notion, finding that a more particularized showing of harm is necessary.[13] In other words, courts in the former jurisdictional group have prioritized the protection of individual plaintiffs in data breach cases, whereas those in the latter group lean toward protecting defendant corporations. In order to assess whether to confer standing,

---

Marcello Antonucci *is the Global Cyber & Tech Claims Team leader on the Cyber & Executive Risk Team at Beazley Group in Chicago. He is experienced in data privacy and cybersecurity matters, including guiding policyholders through immediate and comprehensive responses to data breaches and network intrusions; managing claims and regulatory investigations arising out of privacy breaches; and managing claims arising out of tech errors and omissions, intellectual property, and media and advertising liability.* **Jana Landon** *is an associate vice president and senior counsel in the Privacy Group at Lincoln Financial Group in Radnor, Pennsylvania. She manages data privacy incident response and consults with Lincoln business units on a diverse range of privacy issues and initiatives, including compliance with new regulations, data privacy agreements, and best practices involving use of emerging technologies. She holds a CIPP/US designation from the International Association of Privacy Professionals. Landon would like to thank Joshua Lesser for his contribution to this article.* **Chad Layton** *is a shareholder in the Chicago office of Segal McCambridge Singer & Mahoney, Ltd., and serves as a cochair of the firm's Technology and Cyber Risk Practice Group. He is a trial attorney and litigation partner with extensive experience handling commercial litigation, cyber risk, technology errors and omissions, employment, and other litigation matters. Layton would like to thank Sarah Flohr, Nathan Law, and Rachel Laurel for their contributions to this article.* **Darin McMullen** *is a senior vice president and national E&O/cyber product leader with Aon's Professional Risk Solutions Group in Philadelphia, Pennsylvania, where he focuses on cyber insurance product innovation and the development of effective cyber-risk–transfer solutions for Aon clients, with whom he works extensively in reviewing and tailoring policy language to ensure best-in-class coverage. His expertise includes cyber insurance and errors and omissions insurance, as well as analysis of the connectivity between cyber insurance and other lines, including property insurance. They may be reached, respectively, at marcello.antonucci@beazley.com, jana.landon@lfg.com, clayton@smsm.com, and darin.mcmullen@aon.com.*

courts have analyzed the circumstances surrounding the breach, including the congressional intent behind any statutory protection, the type of data that was stolen, and the amount of time that has passed since the breach.

The lack of consensus in the federal courts regarding the circumstances that would confer standing in data breach cases has led to forum shopping.

THE LIBERAL APPROACH: A LOW STANDARD FOR STANDING

Whether standing exists is typically addressed at the outset of a lawsuit, via a motion to dismiss that raises arguments based on the purported insufficiency of the complaint. In some cases involving standing, the concept of legal liability may be presumed at the outset of a case (for the time being), and the focus of the dispute becomes the nature of the plaintiffs' damages as alleged in the complaint.

Some courts are inclined to side with plaintiffs despite the absence of what many legal practitioners would consider to be a concrete harm. For example, in identify theft cases, courts often consider that the heightened risk that identity theft may occur in the future—even if such a theft never actually occurs—is sufficient to confer standing. In other words, courts allow lawsuits to survive motions to dismiss and proceed through expensive discovery and to trial for plaintiffs who are not out of pocket any actual damages.

This approach arguably runs afoul of commonsense notions of fairness. After all, why should a defendant, who itself was likely victimized by a cyberattack, be subject to legal liability to a plaintiff who does not appear to have suffered any true harm?

Third Circuit cases. The Third Circuit found the facts in one data breach case sufficient to confer standing, but the court limited that holding by differentiating and finding no standing in a non–data breach case.

The Third Circuit concluded that standing did exist in *In re Horizon Healthcare Services Inc. Data Breach Litigation*.[14] In that case, the Third Circuit held that alleged violations of the Fair Credit Reporting Act (FCRA) were sufficient to confer standing. Two laptops that contained unencrypted personal information of Horizon members were stolen. The lawsuit did not allege that any identities had actually been stolen. Nonetheless, the court held that, through governing legislation, Congress had established that the unauthorized dissemination of personal information by a credit reporting agency, in and of itself, causes an injury sufficient to establish standing,[15] even though the information is truthful and not harmful to anyone's reputation.[16]

> **In identify theft cases, courts often consider that the heightened risk that identity theft may occur in the future—even if such a theft never actually occurs—is sufficient to confer standing.**

However, in *Kamal v. J. Crew Group, Inc.*,[17] a case not involving a data breach, the Third Circuit limited its holding in *Horizon Healthcare Services*. The consumer plaintiffs in *Kamal* filed suit under the Fair and Accurate Credit Transactions Act (FACTA) against a retailer who printed more than the last five digits of credit card numbers on a receipt. The plaintiffs in *Kamal* alleged "two 'concrete' harms: the printing of the prohibited information itself and the harm caused by such printing increasing the risk of identity theft," an "injury which no doubt involves a technical violation of FACTA's ban on printing more than the last five digits of a consumer's credit card number."[18] In *Horizon Healthcare Services*, the Third Circuit stated that

> under the FCRA Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm. . . .[19]

In *Kamal*, the Third Circuit explained that

> [i]n *Horizon*, it was the alleged injury's close relationship to a traditional harm that showed it was sufficiently concrete to create standing. Here, absent unauthorized third-party disclosure, Kamal's alleged FACTA violation is not "an injury in and of itself." Accordingly, we will evaluate whether the FACTA procedural right protects a concrete interest, and if the violation alleged by Kamal entails a degree of risk sufficient to meet the concreteness requirement.[20]

The Third Circuit concluded that the alleged FACTA violation was merely procedural and did not confer Article III standing.[21]

Ninth Circuit case. The Ninth Circuit in *Ree v. Zappos.com, Inc.*[22] distinguished an Eighth Circuit case,

In re SuperValu, Inc., Customer Data Security Breach Litigation, reasoning that standing turns on the type of data allegedly stolen.[23]

The Ninth Circuit explained that in *SuperValu*, apart from allegations of credit card theft, "no other PII, such as addresses, telephone numbers, or passwords, was stolen."[24] However, in *Zappos.com*, the plaintiffs alleged that hackers had obtained their "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information."[25] Therefore, the court found that "the sum of their allegations in light of *Krottner*" showed that the plaintiffs had "sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft."[26]

D.C. Circuit case. In *Attias v. CareFirst, Inc.*,[27] the D.C. Circuit also found that affected consumers had standing.

CareFirst, a health insurer, suffered a data breach in 2014 that revealed patients' names, birth dates, email addresses, Social Security numbers, and credit card information. The court ruled that a heightened risk of future identity theft, without more, was sufficient to confer standing.[28] It reasoned that it was sufficient that an unauthorized party had accessed personal data, and it was willing "to infer that this party has both the intent and ability to use that data for ill."[29] This conclusion was bolstered by the fact that two of the plaintiffs, Curt and Connie Tringler, alleged that they already had suffered identity theft as a result of the breach.[30]

District court case. Of course, no discussion of standing would be complete without a discussion of Yahoo! and the three multiyear data breaches that resulted in the potential exposure of over one million individuals.

In a 93-page decision in *In re Yahoo! Inc. Customer Data Security Breach Litigation*,[31] U.S. District Court Judge Lucy Koh disagreed with Yahoo!'s contention that breach victims lacked standing to sue, explaining that breach victims could pursue traditional negligence claims as well as claims for breach of contract and unfair competition. The district court explained that the injury-in-fact standing requirement had been met because "[a]ll plaintiffs have alleged a risk of future identity theft, in addition to loss of value of their personal identification information."[32] In further support of its decision, the district court noted that some plaintiffs alleged that they had spent money to ward off future identity theft, that their data had been misused, and that they had lost the benefit of their bargain under the contract.[33]

Non–data breach cases. Two recent non–data breach cases illustrate the trend toward finding standing for consumers and may provide a glimpse into how courts will rule in data breach class actions in the future.

In *Muransky v. Godiva Chocolatier, Inc.*,[34] the Eleventh Circuit was more willing to confer standing than other federal appellate courts for a FACTA violation. While the court agreed that "bare procedural violations, divorced from any concrete harm," do not grant the plaintiff standing,[35] the court expanded the notion of what constitutes concrete harm by stating that "identity theft bears a close enough relationship to the common-law tort of breach of confidence to make [the plaintiff's] injury concrete."[36] The Eleventh Circuit concluded that the concreteness requirement in *Spokeo* can be satisfied by "intangible injuries, including injury in the form of a risk of real harm."[37] Furthermore, according to the court, an injury may even be a "small injury, an identifiable trifle."[38]

The Second Circuit also recently expanded Article III standing to include mere technical violations of the Telephone Consumer Protection Act (TCPA). In *Melito v. Experian Marketing Solutions, Inc.*,[39] the court concluded that the receipt of unwanted text messages in violation of the TCPA was sufficient to confer standing. According to the Second Circuit, the plaintiff "need not allege any *additional* harm beyond the one Congress has identified"; and, thus, the "receipt of unwanted advertisements *is itself* the harm."[40] Contrary to the Third Circuit's ruling in *Kamal*, the Second Circuit determined that a technical violation is sufficient to confer standing absent any additional harm.

THE NARROW APPROACH: A HIGHER STANDARD FOR STANDING

Other courts have taken a narrow approach to standing, finding no standing for plaintiffs under fact patterns similar to the cases discussed above. Courts following the narrow approach to standing in data breach litigation have done so on the basis that the injury-in-fact requirement for standing necessitates not only the misuse of a plaintiff's data but also harm to that plaintiff's personal data. Thus, in trying to obtain standing in these jurisdictions, the plaintiff must plead sufficiently that there is a causal connection between the injury suffered and the data breach. Furthermore, district courts in various circuits have found that *Clapper*'s "certainly impending" standard does not confer standing on plaintiffs who allege only an increased risk of future harm.

The requirement that a plaintiff must have suffered an actual economic harm will, of course, be impossible to establish in some cases. As a consequence, plaintiffs' lawsuits often fall victim to motions to dismiss in those jurisdictions that adhere to the approach espoused by the Fourth Circuit (see below) and other like-minded courts. Thus, any corporate defendant that must defend itself against a data breach

lawsuit should make every effort to obtain jurisdiction in a court that narrowly construes the concept of legal standing.

Second Circuit case. *Whalen v. Michaels Stores, Inc.*[41] is an example of a case in which the court took a narrow approach. In that case, the Second Circuit found that customers whose data had been breached had no standing.

In 2014, Michaels suffered a cyberattack that compromised credit and debit card information for 2.6 million customers. The plaintiff made purchases at Michaels in 2014; shortly thereafter, two attempts were made to make charges to her credit card in Ecuador. However, no charges were actually made. She brought an action for breach of implied contract and for violation of a section of the New York General Business Law.

The district court held that the allegations in the complaint did not suffice to establish Article III standing because Whalen neither alleged that she incurred any actual charges on her credit card nor alleged—with any specificity—that she had spent time or money monitoring her credit. The appellate court agreed, finding that no standing existed and that the injuries alleged were not sufficiently concrete or particularized.

This view has since been adopted by both the U.S. District Court for the Eastern District of New York and the U.S. District Court for the Western District of Kentucky.[42]

Fourth Circuit case. The Fourth Circuit arguably has set the highest standard for Article III standing in data breach cases both at the pleading stage and at summary judgment.

In *Beck v. McDonald*,[43] the Fourth Circuit addressed two consolidated cases involving data breaches at a Veteran Affairs Medical Center: the first was the likely theft of an unencrypted laptop, and the second was the loss or theft of four boxes of pathology reports. The plaintiffs asserted their claims under the Privacy Act of 1974 and the Administrative Procedure Act, alleging that they feared an increased risk of future identity theft and that they would have to incur costs to protect against that risk.

The court held that allegations of an increased risk of identity theft, without allegations that the information had been targeted or accessed, are not sufficient to confer standing. The court also rejected claims that "emotional upset" and "fear [of] identity theft and financial fraud" are sufficient.[44] It declined to follow other circuits that infer a substantial risk of future identity theft from an organization's offer to provide free credit monitoring. Finally, the court held that any mitigation expenses incurred by the plaintiffs were "self-imposed harms [that] cannot confer standing."[45]

Courts following the narrow approach to standing in data breach litigation have done so on the basis that the injury-in-fact requirement for standing necessitates not only the misuse of a plaintiff's data but also harm to that plaintiff's personal data.

Eighth Circuit cases. The Eighth Circuit has ruled that plaintiffs have standing where an actual economic harm has occurred.

In *Kuhns v. Scottrade, Inc.*,[46] for example, the court granted the plaintiffs standing. In 2016, Scottrade customers filed a class action complaint, alleging that between September 2013 and February 2014 hackers accessed Scottrade's databases and acquired sensitive information for 4.6 million customers. The plaintiffs further alleged that Scottrade provided inadequate security in violation of its contractual obligations to protect customers' personal and financial information. The plaintiffs, therefore, faced an imminent and increased risk of identity theft and fraud.

The district court dismissed the action, finding that the plaintiffs lacked standing. The Eighth Circuit, however, found that Kuhns (the only plaintiff that appealed) suffered an injury in fact: "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical."[47] Specifically, Kuhns alleged, Kuhns's payment to Scottrade included information-security services, and "Scottrade breached the contract when it failed to provide promised reasonable safeguards"; thus, "Kuhns suffered . . . the diminished value of his bargain"—in other words, "the difference between the amount he paid and the value of the services received is an actual economic injury that establishes injury in fact for his contract-related claims."[48] The court applied Eighth Circuit authority holding that "a party to a breached contract has a judicially cognizable interest for standing purposes regardless of the merits of the breach alleged."[49] (After it found that the plaintiff had standing, however, the court then determined that the complaint failed to state a claim, so it dismissed the case in its entirety.) District courts sitting in the Eighth Circuit have utilized the *Kuhns* analysis in