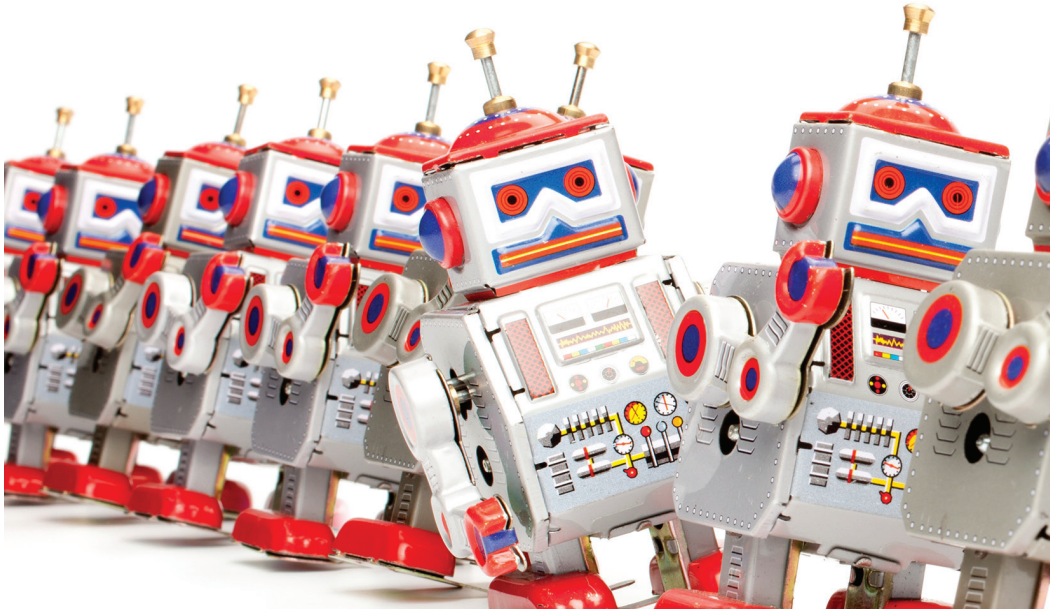
Recent Developments and Trends to Watch

Data Breach Class

By Edward J. Bennett and Matthew H. Blumenstein

As more cases reach the appellate courts, litigants can expect greater clarity in the future about the factors that will affect class certification, but some tendencies have already emerged.



Putative data breach class actions continue to proliferate. While the number and diversity of cases—and inventiveness of counsel and courts—have left the jurisprudence somewhat muddled, certain trends became clearer in 2014 and 2015. For example, plaintiffs generally can expect their claims to be dismissed unless they credibly allege that the named plaintiffs have suffered some sort of actual injury—as opposed to merely an increased risk of injury—*and* that the injury is traceable to the theft of their data from a defendant. As more cases course their way into the appellate courts, litigants can expect greater clarity regarding the factors that will affect whether a given case is to be certified as a class action and survive motions practice. But already the jurisprudence suggests certain steps that defendants and their counsel can take to reduce exposure in the wake of a data breach.

Plaintiffs Allege Diverse Causes of Action

In recent years, courts generally have been somewhat hostile toward putative data breach class actions, regularly dismissing suits for lack of standing or failure to plead claims upon which relief can be granted. *See, e.g.*, *Galaria v. Nationwide Mut. Ins.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) (collecting cases). In response, plaintiffs' counsel have dug deeply into the treatises to craft a menu of novel claims to plead alongside traditional negligence and contract claims—including breach of (implied) contract, negligence, negligent misrepresentation, unjust enrichment, bailment, and violations of sundry state privacy and consumer protection statutes. Some of these theories have survived motions to dis-

■ Edward J. "Ted" Bennett is a partner with Williams & Connolly LLP in Washington, D.C. His practice focuses on trial work and complex civil litigation, principally in the banking, securities, financial services, and patent fields. Mr. Bennett is a member of DRI. Matthew H. Blumenstein is an associate with Williams & Connolly LLP in Washington, D.C. His practice focuses on complex civil litigation and white-collar criminal defense.

Action Litigation

miss, and many others have not. Until there become clear winners and losers, however, defendants can expect plaintiffs to throw the proverbial kitchen sink into their complaints.

Judge Klausner explored several theories of liability in the *Sony* litigation, which arose out of the theft of personally identifiable information (PII) concerning more than 15,000 Sony employees. *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex.), 2015 WL 3916744 (C.D. Cal. June 15, 2015). The plaintiffs alleged that because of the theft they were forced to "purchase identity protection services and insurance, and take other measures to protect their compromised PII." *Id.* at *1. The plaintiffs also alleged that "[n]otwithstanding these measures, [they] face ongoing future vulnerability to identity theft, medical theft, tax fraud, and financial theft because their PII has been, and may still be, publicly available to anyone with an internet connection." *Id.* Importantly, the *Sony* plaintiffs were also able to allege that their "PII has already been traded on black market websites and used by identity thieves." *Id.* Because their data had been not only exposed to misuse but actually misused, the plaintiffs alleged an assortment of harms supposedly caused by the data theft:

> (1) loss of opportunity to control how their PII is used; (2) diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft or unauthorized use of financial and medical accounts; (5) lost opportunity costs and loss of productivity from efforts to mitigate the actual and future consequences of the breach; (6) costs associated with the inability to use credit and assets frozen or flagged due to credit misuse; (7) unauthorized use of compromised PII; (8) tax fraud or other unauthorized charges to financial, health care or medical accounts; (9) continued risk to the PII that remain in the possession of Sony, as long as Sony fails to undertake adequate measures; and (10) future costs in terms of time, effort, and money that will be expended to prevent and repair the impact of the data breach.

Id.

The court held that the plaintiffs had standing (discussed below) and that they had adequately pled negligence—*i.e.*, a breach of Sony's "duty to implement and maintain adequate security measures to safeguard its employees' PII," to the extent that their claim was based on "costs relating to credit monitoring, identity theft protection, and penalties." *Id.* at *3–5. Moreover, to overcome the economic-loss doctrine, which generally prohibits recovery of purely economic losses based on negligence, the court held that the plaintiffs had adequately pled a special relationship with their employer, Sony. *Id.* at *5. (Other courts have held that consumers, as opposed to employees, lack a special relationship with defendants and have dismissed data breach negligence claims arising under the economic loss doctrine.)

The *Sony* court dismissed the negligence claim, however, insofar as it was based on "Sony's alleged duty to timely notify." *Id.* The court also held that allegations of "future harm or an increased risk in harm that has not yet occurred… do not support a claim for negligence, as they fail to allege a cognizable injury." *Id.* at *4. Likewise, the court rejected claims based on the diminution of the value of the plaintiffs' PII because the plaintiffs failed to establish that their PII had "compensable value in the economy at large." *Id. See also In re Zappos.com Inc. Cust. Data Sec. Breach Litig.*, No. 3:12-CV-00325-RCJ-VPC, 2015 WL 3466943, at *3, ____F. Supp. 3d.____ (D. Nev. June 1, 2015). The court also dismissed claims for breach of implied contract and statutory claims under California, Virginia, and Colorado law but sustained claims under California's Confidentiality of Medical Information Act and Unfair Competition Law. *Corona*, 2015 WL 3916744, at *6–9.

In other consumer class actions, plaintiffs often also seek to plead claims for unjust enrichment, alleging that they would not have purchased goods or services from a defendant had they known that their data would become vulnerable. *See, e.g.*, *In re Target Corp. Cust. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177–79 (D. Minn. 2014). While the court in *Target* held that the plaintiffs had adequately pleaded unjust enrichment, other courts have questioned the viability of this theory, as in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 695 (7th Cir. 2015), or they have outright rejected claims invoking it. *See, e.g.*, *Carlsen v. Gamestop, Inc.*, No. 14-3131 (DFW/SER), 2015 WL 3538906, at *8, ____F. Supp. 3d.____ (D. Minn. June 4, 2015).

Standing Continues to Pose a Significant Hurdle

Standing continues to be a substantial barrier to federal class actions, with some plaintiffs even invoking their *lack* of federal standing in an attempt to escape Class Action Fairness Act (CAFA) removal. Most commonly, courts that have dismissed class actions for lack of standing have cited the plaintiffs' inability to adequately allege that a data breach actually caused them to be injured. A recent decision by the Seventh Circuit, however, may provide an opening for some plaintiffs.

Relying on the U.S. Supreme Court 2013 decision in *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013), federal courts increasingly have been dismissing class actions for want of Article III standing, holding that plaintiffs whose stolen data has not yet been misused have failed to prove injury in fact. While some courts have held that *Clapper* did not overrule the broadly accepted standard that plaintiffs must allege "real and immediate" harm to establish standing, other courts have interpreted *Clapper's* "clearly impending" standard to set a higher bar. Irrespective of whether *Clapper* changed the law, courts interpreting it have regularly dismissed cases when none of the plaintiffs had yet suffered credit card or other fraud as a result of the data theft. *See*, *e.g.*, *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015). And even in cases when some plaintiffs had been injured, courts generally have held that the harm cannot be plausibly traced to the defendant if the incidents of harm among the plaintiffs are too infrequent or too distant in time from the hack. *See, e.g.*, *In re Zappos.com Inc. Cust. Data Sec. Breach Litig.*, 2015 WL 3466943, at *9; *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *8, While some courts have held that *Clapper* did not overrule the broadly accepted standard that plaintiffs must allege "real and immediate" harm to establish standing, other courts have interpreted *Clapper's* "clearly impending" standard to set a higher bar. No. 13-7418 (CCC) (D.N.J. Mar. 31, 2015) (no causation where only one out of 839,000 affected customers claimed to have suffered a financial fraud); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 32 (D.D.C. 2014) (plaintiffs cannot show causation because, among other things, "[i]n a society where around 3.3 percent of the population will experience some form of identity theft—regardless of the source—it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud"). In addition, courts have held standing to be lacking when the potential future harm, such as bank or credit card fraud, would occur only if an independent third party took some action with the plaintiffs' PII. *See, e.g.*, *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *6 (collecting cases).

Plaintiffs who have yet to suffer credit card or other fraud have tried—usually unsuccessfully—to establish injury in fact by claiming that the theft of their PII diminished its value. Even when plaintiffs were able to allege that their PII had value on the black market, courts frequently have found that they failed to plausibly allege that its value *to them* had been diminished. Similarly, uninjured plaintiffs who paid for fraud-monitoring or protection services after a hack generally have not been successful in leveraging those expenses as an independent basis for standing. Instead, courts, citing *Clapper*, have found those costs to be cognizable injury only when fraud was "clearly impending"—and thus standing was not proper irrespective of the payments. *See*, *e.g.*, *Green*, 2015 WL 2066531, at *5.

The Seventh Circuit July 2015 decision in *Remijas v. Neiman Marcus* seems to buck this trend. Reversing the trial court, the court of appeals held that the Neiman Marcus customers who had their PII stolen by hackers had established Article III standing because (1) there was an "objectively reasonable likelihood" that they would suffer identity theft or credit card fraud in the future, and (2) they already had spent time and money remediating their exposure to fraud. 794 F.3d at 693 (internal quotation marks omitted). Unlike plaintiffs in many cases, however, the plaintiffs in *Remijas* were able to rely on the fact that 9,200 of the 350,000 customers whose data was stolen already had suffered some sort of fraud. In the court's opinion, this made the threat of future harm much more imminent and less theoretical. A practitioner can expect that plaintiffs will rely heavily on *Remijas*, as well as on *In re Adobe Systems Inc. Privacy Litigation*, 66 F. Supp. 3d. 1197 (N.D. Cal. 2014), in which the court found standing under similar circumstances.

In addition, data theft plaintiffs undoubtedly will continue to analogize their claims to toxic tort jurisprudence; courts in toxic tort cases have found standing for uninjured plaintiffs who face an increased risk of harm, such as those who were exposed to a dangerous substance and sought medical monitoring. *See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) ("[T]he 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.") (footnote omitted); *Cent. Delta Water Agency v. United States*, 306 F.3d 938, 947–48 (9th Cir. 2002) (holding that "the possibility of future injury may be sufficient to confer standing on plaintiffs" and noting that "threatened injury constitutes injury-in-fact" (internal quotation marks omitted)); *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000) (en banc) ("Threats or increased risk… constitutes cognizable harm."). *See also Sutton v. St. Jude Med. S.C., Inc.*, 419 F.3d 568, 574–75 (6th Cir. 2005) (concluding that standing was present where a defective medical implement presented an increased risk of future health problems); *Carlough v. Amchem Prods., Inc.*, 834 F. Supp. 1437, 1452 (E.D. Pa. 1993) (holding that plaintiffs who were exposed to asbestos but had not yet developed asbestos-related conditions had standing to bring suit for injuries).

Intra-Class Differences Continue to Hinder Class Certification

Whether or not plaintiffs have suffered injury-in-fact and whether or not their injuries are traceable to a defendant's hack—questions that bedevil plaintiffs during the standing stage—can be barriers to class certification as well. Customer classes tend to have a mixture of plaintiffs who have suffered some tangible harm and those who have not. And some plaintiffs' injuries may be more readily traceable to a data breach than others because they occurred closer in time or because other plaintiffs may have suffered other, unrelated thefts that could have caused their harm. Also, data breach class actions are likely to involve the laws

of many different states—an issue that is pending before the U.S. District Court for the District of Minnesota, as credit card issuers from several states seek class certification against Target for losses arising out of the notorious theft of its customers' data. *See In re Target Cust. Data Sec. Breach Litig.*, 66 F. Supp. 3d. 1154 (D. Minn. Dec. 2014). All of these factors may prove to be challenging to plaintiffs who survive initial challenges to standing and the plausibility of their claims. *But see Tabata v. Charleston Area Med. Ctr., Inc.*, 759 S.E.2d 459 (W. Va. 2014) (*per curiam*) (class certified).

What to Watch for in 2016

While this area of law continues to evolve in courthouses throughout the country, a few matters warrant particular attention. First, in the coming term the Supreme Court will decide *Spokeo v. Robins*. The question presented in that case is whether Congress can confer Article III standing based on a so-called statutory injury, in the absence of concrete harm. Although the case concerns purported violations of the Fair Credit Reporting Act, and not data breach litigation per se, the court's decision has the potential to curtail or expand data breach class actions dramatically based on alleged statutory injuries. If the Supreme Court disclaims Article III standing based solely on statutory injuries, then data breach plaintiffs' lawyers will be required—and often hard pressed—to demonstrate that class members suffered injuries that are (1) concrete and (2) sufficiently similar to support commonality and predominance. Conversely, if the Court holds that statutory violations are sufficient to satisfy Article III's injury requirement, then data privacy statutes will serve as ready-made sources of undifferentiated injuries for the purpose of class certification.

On the crucial subject of injury more generally, we should watch for other courts' reactions to *Remijas*, 794 F.3d 688, in which the Seventh Circuit held, among other things, that the plaintiffs adequately alleged imminent injuries in the form of "an increased risk of future fraudulent charges and greater susceptibility to identity theft." *Id.* at 692–94. As of this writing, Westlaw and Lexis contained one data breach brief grappling with *Remijas*: the corporate defendant in *In re Supervalu, Inc. Customer Data Security Breach Litigation*, No. 14-MD-2586, attempts to distinguish *Remijas* in its August 10, 2015, motion to dismiss for lack of standing. More such briefs are virtually certain to follow, along with a flurry of decisions dealing with the Seventh Circuit's holding.

Also, on November 10, 2015, the Supreme Court was scheduled to hear argument in *Tyson Foods, Inc. v. Bouaphakeo*, which likely will affect data breach litigation by informing courts' analyses of the commonality and predominance requirements in cases for which there is a mix of injured and uninjured plaintiffs. In *Bouaphakeo*, the district court and Eighth Circuit held that the plaintiffs satisfied Rule 23(b)(3) even though the plaintiffs' expert conceded that over 200 class members suffered no injury. One of the questions before the Supreme Court, therefore, is whether a class action may be certified under Rule 23(b)(3) "when the class contains hundreds of members who were not injured and have no legal right to any damages." The Court's answer to that question will sound throughout the class action universe, including especially data breach litigation, where some plaintiffs may have suffered credit card or identity fraud, while others may not have.

Finally, the *Target* litigation continues to be worth watching, as it is the most advanced large-scale data breach case to date. Judge Manguson of the U.S. District Court for District of Minnesota oversees this multidistrict litigation, which includes a settlement class for consumers and a separate class for financial institutions. The consumer class consists of an estimated 110 million members. The complaint includes claims under state consumer protection and data breach statutes, negligence, breach of contract, bailment, and unjust enrichment. In December 2014, the court mostly denied Target's motion to dismiss, notably rejecting the argument that the putative class members lack Article III standing because they cannot establish injury. Then, in March 2015, the court preliminarily approved a settlement requiring Target to pay $10 million for consumers' claims and up to $6.75 million in attorneys' fees. Under the agreement, class members who can document losses each will be eligible for up to $10,000, and class members who cannot document losses will share equally in any remaining settlement funds. The proposed settlement also requires Target to undertake new measures to enhance its data security. A final approval hearing was set for November 10, 2015.

Plaintiffs in the financial institution class action against Target include banks and credit unions that issued allegedly compromised debit or credit cards. The complaint claims negligence, negligence per se, and violation of Minnesota's Plastic Security Card Act. The issuing banks seek compensation for the costs of replacing cards, reimbursing customers for fraudulent transactions, and related expenses. In December 2014, the court largely denied a motion to dismiss, holding, among other things, that Target's relationship with the issuing banks gave rise to a duty of care. And the court certified the class in September 2015, holding, among other things, that (1) "Plaintiffs have established for the purposes of the class-certification inquiry that they suffered injury proximately caused by the data breach"; (2) Plaintiffs have established that "it is possible to prove classwide common injury and to reliably compute classwide damages resulting from reissuance costs and fraud losses" (and if classwide damages prove unworkable, a damages class can be decertified and damages questions stayed for determination after the liability phase concludes"); and (3) Plaintiffs' statutory claim is susceptible to classwide proof. Slip Op. 7–13. Stay tuned.

One of the questions before the Supreme Court, therefore, is whether a class action may be certified under Rule 23(b)(3) "when the class contains hundreds of members who were not injured and have no legal right to any damages."