CORPORATE COUNSEL
An ALM Website
corpcounsel.com | July 25, 2017

# Once More Unto the Breach: A Discussion of Recent Data Breach Litigation

*Edward J. Bennett, Matthew H. Blumenstein and Xiao Wang*

$115 million. 80 million class members. 120 lawsuits.

These three numbers capture only a small part of the story in *Anthem*, a multidistrict data breach litigation before Judge Lucy Koh in the Northern District of California. Last month, the *Anthem* parties agreed to settle all claims for $115 million—a new record for data breach cases (by comparison, data breach cases against Target and Sony Pictures settled for $18 and $3 million, respectively).

The *Anthem* settlement appears to represent yet another watershed moment in data breach litigation. This is a still a relatively new and rapidly evolving field, but, as more and more of these cases are filed, several recurring battle lines have emerged through parties' arguments and judicial opinions. This article discusses two such issues—standing and class certification. It also discusses the prospect of additional clarity in this area.

*Credit: supimol kumying/Shutterstock.com*

## Standing

Data breach plaintiffs commonly allege two types of harm. First, plaintiffs allege an increased risk of identity theft, and seek compensation for out-of-pocket costs such as credit monitoring. Second, plaintiffs seek benefit of the bargain losses, claiming that they paid for but did not receive adequate data security. Under both theories, however, plaintiffs must show injury and causation to establish standing—requirements which have, thus far, generally represented stumbling blocks for data breach litigants.

• Increased Risk of Identity Theft

Many courts have dismissed cases where no plaintiff has suffered harm as a direct result of the breach, even if plaintiffs have paid out of pocket costs to protect themselves from possible injury. As the Fourth Circuit observed in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), for merely "speculative threats," self-imposed costs "cannot confer standing."

The Seventh Circuit's decision in *Remijas v. Neiman Marcus Group,* 794 F.3d 688, 693 (7th Cir. 2015), however, bucked that trend. There, the court held that customers who had their personal information stolen "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 ...

injury will occur." Unlike plaintiffs in Beck, however, the *Remijas* plaintiffs noted that 9,200 of the 350,000 customers at issue had already suffered some sort of fraud. This, in the court's view, made the threat of future harm imminent, rather than speculative.

• Benefit of the Bargain Losses

Plaintiffs have also asserted a "benefit of the bargain" damages theory. In *Resnick v. AvMed*, 693 F.3d 1317, 1328 (11th Cir. 2012), for instance, the Eleventh Circuit denied dismissal where plaintiffs alleged (1) that "they conferred a monetary benefit ... in the form of monthly premiums," (2) that defendant claimed that he had used these premiums to "pay for ... data management and security," and (3) that defendant had "failed to implement ... measures ... mandated by industry standards."

Most courts, however, have rejected this theory, "because ... plaintiffs fail to explain how a data breach affected the value of the goods they purchased," *Chambliss v. Carefirst*, 189 F. Supp. 3d 564, 572 (D. Md. 2016). In particular, these courts have focused on whether plaintiffs have made any "factual allegations indicating that the prices they paid for [a service] included a sum to be used for data security."

**Class Certification**

Whether plaintiffs have been injured—an essential standing issue—can also serve as a barrier to class certification. Although only a handful of data breach cases have reached class certification, those that have generally include classes with a mix of individuals who have suffered some tangible harm (such as identity theft) and those who have not.

Indeed, this mix of injuries led the Eighth Circuit to reverse the district court's class certification decision in Target, finding that the district court had not sufficiently examined whether the lead plaintiff was an adequate representative for the putative class, as in *In re Target Customer Data Security Breach Litigation*, 847 F.3d 608, 613 (8th Cir. 2017). On remand, the Eighth Circuit specifically instructed the district court to consider "whether an intraclass conflict exists when class members who cannot claim money from a settlement fund are represented by class members who can."

**Looking Ahead**

As is evident from the discussion above, data breach cases have engendered a number of disagreements amongst the courts. Indeed, at present, four circuits—the First, Second, Third, and Fourth—have concluded that an increased risk of identity theft may establish injury sufficient for standing, while three—Sixth, Seventh, and Ninth—have held otherwise. This split, alongside other emerging issues, may presage clarification from the Supreme Court. In the absence of such clarification, however, circuit court decisions, including those concerning the legal arguments discussed here, will guide how putative data breach actions are litigated going forward.

***Ted Bennett*** *is a partner at Williams & Connolly. His practice focuses on trial work and complex civil litigation, principally in matters relating to banking and financial services, and patents, trade secrets and other intellectual property.* ***Matt Blumenstein*** *is an associate at the firm. He handles a wide variety of litigation, with an emphases on complex civil litigation and white collar criminal defense. He has represented companies and individuals in federal and state courts across the country.* ***Xiao Wang*** *is an associate at the firm. His practice focuses on media and entertainment, electronic privacy and securities litigation.*