CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | February 16, 2022

Data Breach Class Action Litigation Trends To Watch in 2022

By David Balser, Susan Clare and Elizabeth Adler

Given the increased frequency of data breaches and the high-stakes class action litigation that often follows, it is critical for counsel to be aware of the key issues that corporate defendants are currently facing in this fast-evolving space. Below we discuss three hotly litigated issues that we expect will continue to be at the forefront of data breach litigation and important to follow this year.

Article III Standing Challenges

When the U.S. Supreme Court issued its decision in *TransUnion v. Ramirez* in June 2021, it appeared to mark a watershed moment in class action practice in federal courts. Counsel specializing in data breach litigation have anticipated that *Ramirez*'s holding—that a mere "risk of harm" cannot confer standing to seek damages—will undercut the key injury theory of risk of identity theft that has been ubiquitous in data breach litigation for years. But while *Ramirez* has been thoroughly analyzed by legal commentators, courts are only beginning to define its contours. Moreover, the courts that have considered the "risk of harm" issue post-*Ramirez* have come to different conclusions, making it difficult to predict *Ramirez's* reach and an area to watch in 2022.

Thus far, some courts addressing *Ramirez* in data breach cases have been hesitant to read the decision as a sea change in standing law. For example, the District of South Carolina in *In re Blackbaud Customer Data Breach Litigation* recently distinguished *Ramirez* on procedural grounds. There, the plaintiffs alleged they were at an increased risk of harm following a ransomware attack. The court reasoned that unlike in *Ramirez*, where the case had proceeded through trial, the *Blackbaud* plaintiffs were entitled at the pleading stage to rest on their mere allegation of a risk of harm.

Other courts have declined to discuss *Ramirez* altogether, despite similar allegations of risk of harm. For example, in *In re GE/CBPS Data Breach Litigation*, the Southern District of New York held that a mere risk of identity theft *was* sufficient to confer standing. And even though the court allowed briefing on *Ramirez*, it did not discuss the case in denying defendant's motion to dismiss.

In contrast, in *Legg v. Leaders Life Insurance Company*, the Western District of Oklahoma relied on *Ramirez* in dismissing a case alleging a risk of future harm. The court noted that in light of *Ramirez*, it "is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft following a data breach is still good law, at least with respect to a claim for damages." A Western District of New York magistrate judge reached a similar conclusion in *Tassmer v. Professional Business Systems*, recommending dismissal in the absence of alleged *actual* fraud.

It is yet to be seen if the Supreme Court will clarify whether its holding in *Ramirez* was intended to foreclose a plaintiff's ability to *ever* establish standing to sue for damages based on a risk of harm. However, there is some indication that *Ramirez*'s holding means what is says and should not be limited to its facts. Specifically, the Supreme Court recently ordered the Fourth Circuit to reconsider a class certification order in *Rocket Mortgage v. Alig* in light of *Ramirez*. How the Fourth Circuit resolves the case on reconsideration may be a strong early indication of *Ramirez*'s reach.

While the impact of *Ramirez* is being sorted out, data breach litigants will need to grapple with multiple strategic decisions, including whether and when to raise Article III standing challenges. A dismissal in federal court has obvious potential upside. However, litigation in state

courts with less stringent standing requirements may not be an attractive alternative. How these competing interests play out over the next year is likely to define the data breach litigation landscape for the foreseeable future and deserves close attention.

Novel Damages Theories

While it remains to be seen if *Ramirez* will fundamentally change federal standing law, the current state of uncertainty will likely cause data breach plaintiffs to move away from the ubiquitous "risk of harm" and instead rely on other, more novel injury theories. For instance, plaintiffs may pivot to the theory that personal information has some inherent value for which they need to be compensated after a data breach. Newer cases like *In re Capital One Data Security Breach Litigation*, *Adkins v. Facebook*, and *Springmeyer v. Marriott* have increasingly focused on this theory.

Additionally, in light of *Ramirez*'s focus on "traditional harms" in analyzing standing, plaintiffs are seizing on comparisons between disclosure of their information and traditional privacy torts and breach of contract claims. Because nominal damages may be presumed for such claims, plaintiffs may increasingly advance the theory that each putative class member can individually recover nominal damages—thus creating the risk of aggregate damages that are far from "nominal."

While post-*Ramirez* law continues to mature, defendants in data breach cases should expect to see these types of novel injury theories with increasing frequency. Their novelty will make litigation even more unpredictable because there may be no clear precedent to rely on in gauging a defendant's exposure. Considering these complexities, it is important for counsel to stay apprised of how the law is evolving in various jurisdictions.

Post-Breach Investigations and Privilege

With increasing frequency, courts are rigorously analyzing whether incident response materials, specifically reports and materials created by third-party consultants and forensic investigators, are protected as privileged or work product. Several courts have addressed the topic recently and the trend is likely to continue in 2022 given that such reports are a major target of discovery in data breach litigation.

In several cases, courts have concluded that incident response materials were not shielded from discovery because they were created primarily for the business purpose of improving a company's cybersecurity. For example, forensic reports in the *Rutter's Data Security Breach Litigation*, *In re Capital One Data Security Breach Litigation*, and *In re Dominion Dental Services* were held to be discoverable. But under similar facts, other courts have found incident response materials to be protected: *In re Arby's* and *In re Experian Data Breach Litigation* are two such examples.

When considering such privilege challenges, courts have scrutinized the nature of the services a consultant provides for a company, how those services were described in the services agreement, and whether the consultant previously performed similar services for the defendant. Additional considerations include whether the materials were focused on the remediation of the breach rather than the company's ensuing litigation, other indications that the materials were used for business purposes, and distribution of the materials outside the legal department.

Due to the increased scrutiny and evolving law, companies should consider proactively developing a privilege protocol to inform the company's immediate actions after a breach to maximize the likelihood of protection. This protocol should balance the business need to remediate the breach with the importance of protecting privileged materials. An effective protocol will involve close cooperation between business leadership, the IT and security departments, and in-house and external counsel. It should also include a review process to identify any needed updates to account for case law developments over the course of the year.

David Balser, **Susan Clare** *and* **Elizabeth Adler** *are partners with King & Spalding and have extensive experience defending clients in data breach actions. Mr. Balser leads the firm's nationwide class action practice. King & Spalding associates* **Robert Griest** *and* **Daniel Sanders** *assisted in the preparation of this article and are members of the firm's Trial & Global Disputes practice group.*