July 3, 2023

First Circuit Dives Into Standards for Concrete Harm in Data Breach Litigation

Client Bulletins

Author: **David M. Krueger**

In the complex and rapidly evolving landscape of data breach litigation, the First Circuit's recent case of *Webb v. Injured Workers Pharmacy, LLC* stands as a significant milestone, and it offers a wealth of insights for businesses navigating the intricacies of data security, consumer interactions, and legal standing.

In 2021, the defendant Injured Workers Pharmacy, LLC (IWP), a specialized pharmacy service, suffered a data breach that compromised patients' personally identifiable information (PII). The PII, which included patient names and Social Security numbers, was stolen by cybercriminals who infiltrated IWP's patient records systems and remained undetected for almost four months. Two patients, Alexsis Webb and Marsclette Charley, filed a putative class action against IWP raising a host of claims under various state laws.

The crux of the decision, and the aspect that makes this case noteworthy, revolved around a question of legal standing. Specifically, the court was tasked with determining whether the plaintiffs, as victims of the data breach, had suffered an injury in fact sufficient to confer Article III standing.

In the legal world, the concept of standing is fundamental. It refers to the requirement that a plaintiff must have a sufficient connection to the harm caused by the violation of a law to sue for that violation. In this case, the court found that the plaintiffs had standing to pursue their claims based on two types of injuries: the loss of time and the risk of future harm.

The First Circuit held that the plaintiffs' allegations of spending considerable time and effort monitoring their accounts to protect themselves from identity theft constituted a concrete injury. The court also found that the plaintiffs had plausibly demonstrated a material risk of future harm, given the nature of the stolen PII and the fact that at least some of the stolen PII had already been misused to file a fraudulent tax return in Webb's name. The court found that whether Charley had alleged concrete harm was "more difficult" because, unlike Webb, Charley did "not allege actual misuse" of the PII. But the court concluded that given the nature of the data breach—i.e., cybercriminals intentionally gathering data—there was a natural inference of malicious purpose and "material risk of future misuse" that at least made it plausible that Charley suffered the alleged damage.

There are, however, three caveats with the First Circuit's decision. First, the court also made it clear that a material risk of future harm can satisfy the concrete-harm requirement only as to injunctive relief, not damages. To have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a separate concrete harm caused by their exposure to the risk itself. Thus, while the court found that the plaintiffs had alleged concrete harm solely for purposes of Article III standing, the court expressly did not address whether the plaintiffs had alleged a cognizable distress claim on the merits (an issue the district court never addressed).

Second, the court expressly noted that it was not addressing whether a breach and exposure of PII, *by itself*, constituted an "intangible harm." Finally, and relatedly, the court also made clear that its decision did not apply to a "diminution in value" theory based on PII disclosure, a common damage

claim in data breach litigation. Ultimately, the First Circuit noted that the outcome was dependent on the specific facts of the case, concluding: “We do not hold that individuals face an imminent and substantial future risk in every case in which their information is compromised in a data breach.”

Regardless, despite the First Circuit’s caveats, the *Webb* ruling is significant because it expands the understanding of what constitutes an “injury in fact” under Article III in the context of data breaches. The court’s decision could potentially pave the way for a broader range of plaintiffs to bring claims in data breach cases, even if they have not yet suffered actual identity theft or financial loss. And despite the guardrails the First Circuit attempted to put on its decision, plaintiffs’ attorneys will invariably seek to expand *Webb*’s scope even further.

Businesses should take note of this ruling and review their data security practices to ensure compliance with data protection laws, and consider the implications of *Webb* in relation to any ongoing data breach litigation. When in doubt, consult with your legal counsel to ensure your practices align with the evolving legal landscape. Stay informed, stay compliant, and navigate the data security regulations with confidence.

For more information on this topic, contact David M. Krueger at dkrueger@beneschlaw.com or 216.363.4683.

Related Practices

Litigation

Related Professionals

David M. Krueger
Co-Chair, Privacy Litigation & Compliance Practice Group; CIPP/US
Litigation

T. 216.363.4683
dkrueger@beneschlaw.com