Q: Could You Be Dragged Into Court For A Company Data Breach? A: It Depends

Insights
5.01.17

This same time last year, many in the business community were eagerly anticipating the U.S. Supreme Court's ruling in *Spokeo, Inc. v. Robins*, which was to decide the standard that should be applied to determine whether plaintiffs have standing to sue companies for alleged wrongdoing. Because the outcome would likely impact data breach class action lawsuits, many attorneys who handle data breach litigation paid especially close attention to the case.

Unfortunately, the Supreme Court, operating with only eight justices at the time, remanded the case back to the appeals court in May 2016, finding the lower court's analysis to be incomplete because of its failure to consider whether the plaintiffs' alleged injuries were both concrete and particularized. In the wake of this non-decision decision, lower courts across the country have been split on the issue of whether individuals are able to sue when their personal information is stolen in a data breach incident.

Spokeo And Standing
Spokeo, Inc. operates a "people search engine," that gathers information about individuals and generates background reports about them upon request. The plaintiff sued Spokeo after learning that one such report contained information about him that was inaccurate. He filed the suit as a class action, hoping that anyone else who fell victim to such errant reporting could join his claim.

The Supreme Court was asked to rule on whether the plaintiff and others who wished to join his claim had "standing" under Article III of the Constitution (the legal right to pursue a federal lawsuit), given the fact that the plaintiff did not allege – nor could he demonstrate – he sustained any actual harm, or "injury in fact," due to the incorrect report. Instead, he simply argued that Spokeo committed a technical violation of the Fair Credit Reporting Act, and therefore should be liable to him for damages.

The Court's ruling was considered a "punt" of the issue because it held that plaintiffs must show they suffered an "injury in fact" from the company's alleged wrongdoing to pursue a lawsuit, but then kicked the case back to the lower court to examine the issue anew. The Court emphasized plaintiffs needed to show they suffered a "concrete" injury, but not necessarily a "tangible" injury, stating that even an "intangible injury can nevertheless be concrete."

How Has This Ruling Affected Data Breach Claims?

How Has This Ruling Affected Data Breach Claims?

This ruling seems to have led to more questions than answers, especially in the data breach arena, largely because the circumstances of a company data breach can vary widely. Some plaintiffs allege they lost money as a result of unauthorized use of their credit cards, while others simply allege being forced to spend time and money monitoring their credit because of the risk of a stolen identity is enough to justify a lawsuit. The primary discrepancy among the federal appellate circuits is whether plaintiffs can properly bring a court case based solely on the risk that hackers might misuse personally identifiable information.

In September 2016, the 6th Circuit held in *Galaria v. Nationwide Mutual Insurance Co.* that theft of customers' personal data alone was enough to satisfy the "injury in fact" requirement because it placed them at a continuing and increasing risk of fraud and identity theft. Similarly, in an April 2016 case, the 7th Circuit determined it did not matter whether customer data was actually exposed or misused when it allowed a credit card breach case to proceed.

In contrast, the 3rd and 4th Circuit Courts have not conferred standing to plaintiffs in data breach cases, deeming the "chain of assumptions" required in determining whether an actual injury exists to be too tenuous. As one court described it, *if* the hacker read and understood the plaintiffs' personal information, and *if* the hacker intends to commit future criminal acts, and *if* the hacker is able to use such information to the plaintiffs' detriment, only then would there be an injury in fact. The court held that such a speculative chain of events was too shaky a foundation upon which to build a class action case.

In many cases, such as the February 2017 decision in *Fero v. Excellus Health Plan, Inc.* out of the Western District of New York, the court will determine that standing exists if customer data is stolen and misused, but will decline to do so if there is no allegation of actual misuse. Similarly, in *Beck v. McDonald*, the 4th Circuit determined standing existed when "the data thief intentionally targeted the personal information compromised in the data breaches," and the plaintiffs alleged "misuse or access of that personal information by the thief." The plaintiff in *Beck* made no such assertions, leading to a dismissal of the claim. A 7th Circuit Court case, *Remijas* v. *Neiman Marcus Group, LLC*, was particularly distinguishable; hackers stole credit card information from 350,000 customers and 9,200 of them experienced fraudulent charges, leading to a relatively easy decision from the court to permit the claim to proceed.

What Should You Do?

Now that the Supreme Court has a ninth justice, it's uncertain if and when it will reconsider the issue or resolve the circuit split on standing. The conflict is likely to persist until the Supreme Court revisits the issue and provides more concrete guidance. In the meantime, facing the uncertain landscape in the wake of *Spokeo*, you should continue to be vigilant and exercise care to maximize defenses and promptly respond to data breach incidents.

There are many proactive steps you can take to protect your company: identify the personal, sensitive, and regulated data in your possession and limit access to only those who need it; dispose

of unnecessary information; review security protocols and update them regularly (including maintaining current security software updates); encrypt data at rest and in transit whenever possible; provide training on how to handle and protect your company's data to employees who have access to sensitive information; and create an incident response plan to address data loss when it occurs. Additionally, to the extent you entrust sensitive data to third-party vendors, you should define security standards for them and take steps to ensure they are maintaining adequate security protocols.

You should also consider purchasing cybersecurity insurance to potentially reduce costs in the event of a data breach. If a breach occurs, notify your incident response team and work with your IT department or external security vendor to identify the source of the breach and prevent further loss of data. It is also wise to hire experienced counsel to guide you through the process of adhering to applicable data breach notification laws when notifying appropriate law enforcement agencies of the breach, and engage a public relations firm to assist with public and customer communications.

For more information, contact the authors at RBoerner@fisherphillips.com (610.230.2132) or KFoxhinkle@fisherphillips.com (303.218.3662).

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Service Focus

Privacy and Cyber