



Sixth Circuit Decision Encourages Lawsuits by Customers and Employees Affected by Data Breaches

Taylor A. Gast

Foster Swift Business & Corporate Law News

October 31, 2016

A recent decision by the U.S. Court of Appeals for the Sixth Circuit (the "Sixth Circuit") may make it easier for plaintiffs to bring costly lawsuits against companies that allow sensitive data to fall into the wrong hands. Most troubling from a company's perspective, the Sixth Circuit used language that some states legally require in data breach notification letters to justify allowing the case to move forward.

BACKGROUND

In *Galaria v. Nationwide Mutual Insurance Co.*, the plaintiffs alleged claims for invasion of privacy, negligence, bailment, and violations of the Fair Credit Reporting Act ("FCRA") stemming from a hack of Nationwide's computer network and breach of personal data. In support of their claims, the plaintiffs alleged that the data breach created an "imminent, immediate and continuing increased risk" that class members would be subject to identity fraud. They also argued that victims of identity fraud "typically spend hundreds of hours in personal time and hundreds of dollars in personal funds" to combat the fraud.

The plaintiffs learned of the data breach via a letter sent by Nationwide that urged recipients to take steps to prevent the misuse of stolen data. These steps included monitoring bank accounts and credit reports, and setting up fraud alerts and placing a security freeze on credit reports. Nationwide also offered a free year of credit reporting and up to \$1 million in identity fraud protection through a third-party provider.

Data breach notification letters are required by many states, though the contents that are required vary by state. The inclusion of cautionary language in a data breach notification letter is viewed by many as a best practice, and is in fact, required under many states' data breach notification laws. For example, in Michigan a data breach notification letter must "remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft." MCL 445.72.

AUTHORS/ CONTRIBUTORS

Taylor A. Gast

PRACTICE AREAS

Business & Tax

Technology Law



The district court dismissed the case after concluding that the plaintiffs lacked standing. However, the Sixth Circuit reversed the decision on appeal for reasons discussed below.

THE APPEAL

The Sixth Circuit began by analyzing the district court's determination that the plaintiffs lacked Article III standing. To have Article III standing, a plaintiff must have:

1. Suffered an injury in fact;
2. That is fairly traceable to the challenged conduct of a defendant; and
3. That is likely to be redressed by a favorable judicial decision.

In stating the "injury in fact" requirement, a plaintiff must have suffered an injury, or an injury must be "imminent." In this case, the plaintiffs did not allege that they had been actually harmed by identity fraud yet, but rather that there was a substantial risk of such fraud occurring in the future.

The Sixth Circuit determined that plaintiffs' "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable injury at the pleading stage of the litigation." In support of its conclusion, the Court pointed to language in the breach notification letter, including that Nationwide offered recipients credit monitoring and identity theft protection.

The Court went on to find the "fairly traceable" and "likely to be redressed" elements of standing satisfied, breaking from decisions in other circuits. Diverging opinions between circuit courts are often ripe for review by the United States Supreme Court, and commentators are already speculating that the Nationwide case might reach the High Court.

TROUBLESOME SIGNS FOR BUSINESSES

The Sixth Circuit's decision may encourage employees and customers to sue companies that fall victim to a data breach. Significantly, language that is often legally required to be included in the breach notification advising affected individuals to take steps to prevent or mitigate misuse of the stolen data was used by the Sixth Circuit to infer injury in fact.

The Court's finding could be a powerful tool for data breach plaintiffs moving forward. Although the case is still pending, Nationwide must now continue to pay for ongoing and costly litigation, simply because it advised its customers to be cautious and provided them with services that may prevent any serious damage done.

At a time when businesses, governments, and individuals are experiencing record numbers of information breaches, the Sixth Circuit's decision could make remedial actions even more expensive.

If you have any questions about data breach prevention or response strategies, please call Taylor at 517.371.8238.