Will Sixth Circuit Decision Further Open Doors to Data Breach Recovery Lawsuits?

Oct 05, 2016

Categories:

Publications

Defendants in putative class action suits filed in federal court attempting recovery for data breaches have generally been successful at obtaining dismissal of the claims before their merits can be considered. This is due to the significant hurdle imposed by the standing requirement under Article III of the U.S. Constitution. Many federal courts have dismissed these claims as lacking Article III standing where the plaintiffs have not alleged a present and ascertainable injury, or an "injury-in-fact." But several of the federal appellate courts have indicated a willingness to find standing in these cases, and the recent decision in *Galaria et al. v. Nationwide Mutual Insurance Co.* has further strengthened the hand of plaintiffs' counsel.

The case concerns a data breach which resulted after hackers breached the computer network of Nationwide Mutual Insurance Company and stole the personal information of 1.1 million of Nationwide's customers. The plaintiffs filed a class action lawsuit seeking to recover for their "imminent, immediate and continuing increased risk" of identity fraud.

The Supreme Court has held that a plaintiff must demonstrate three elements to have "standing" – that is, the right to sue – in federal court: the plaintiff must "(1) have 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."

Injury-in-Fact

As to the first element, the plaintiff must have suffered concrete harm, so that a possible future injury is not sufficient. The Supreme Court in *Clapper v. Amnesty Int'l USA* explained that the threatened injury must be "certainly impending" for there to be injury-in-fact, and found the injury element had been met where there was a

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

"substantial risk" that the harm will occur, which may prompt the plaintiffs to incur costs to mitigate the harm. Relying upon *Clapper*, the Court recognized that a reasonable inference can be drawn that in the case of a data breach the personal information that was stolen will be used by the hackers for illegal and fraudulent purposes. Thus, the Court found there to be a sufficiently substantial risk of harm that justified the plaintiffs incurring mitigating costs. Since Nationwide had only agreed to cover a year of identity theft insurance, but not costs to placing security freezes on credit reports, those expenses were necessary, and were a concrete injury. Additionally, the Court observed that Nationwide recognized the risk of future injury by providing credit-monitoring and identity theft protection insurance for an entire year. It recommended that the victims pursue the security freezes and fraud alerts on their credit reports as well.

Traceability

The Court also had no trouble finding that the injury was fairly traceable to the defendant's conduct, the second element of the standing test. The plaintiffs had alleged Nationwide's inadequate administrative, physical and technological safeguards as the direct cause of plaintiffs' injuries, and such allegations were sufficient to meet the threshold for Article III traceability.

Redressability

Finally, the third element – that the plaintiffs' injury will likely be redressed by a favorable decision – was also easily met. The plaintiffs sought compensatory damages for the injuries they incurred, namely the time and money required to monitor their credit and financial accounts, and a favorable verdict would provide redress.

What the Decision Means

The Sixth Circuit's decision aligns the Court with several other federal circuits who have held that incurring expenses to monitor the increased risk of identity theft is sufficient to meet the injury

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

requirement of Article III standing. A majority of courts have refused to find that the mere act of hacking, or evidence of intrusion or penetration of an organization's system, was sufficient to create a substantial risk of harm. But the Sixth Circuit cited the *Remijas v. Neiman Marcus Group, LLC* opinion in which the Seventh Circuit explained: "Why else would hackers break into a store's database and steal consumers' private information" if not to use it for fraudulent purposes?

Indeed, as a result of the *Galaria* decision, the Sixth Circuit joins the Seventh, Ninth and Eleventh Circuits in applying the three-element standing test to defeat a motion to dismiss and permit a class action seeking damages for a data breach to move forward on its merits. While the plaintiffs in these cases still bear the burden of obtaining class certification and proving the defendant's negligence and other common law claims, unless Nationwide decides to appeal the decision to the Supreme Court, the decision strengthens their efforts to pursue recovery for a data breach in the Sixth Circuit.

Additionally, it is as yet unclear what impact the Court's observations concerning Nationwide's loss mitigation recommendations in its notification letter will have on future claims for recovery. Nevertheless, we still believe it is a prudent practice for organizations who find it necessary to notify of a data breach to include information on how to minimize the risk of fraud and identity theft, and to offer to cover the costs of such mitigation efforts. Subsequent remedial measures are inadmissible to prove negligence under the Federal Rules of Evidence, and should ultimately reduce the adverse consequences, including reputational harm, of a data breach.

For more information, please contact Jane Hils Shea or any other attorney in Frost Brown Todd's Privacy and Information Security Law practice.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons