The Court of Appeals for the Sixth Circuit Lowers the Standing Bar in Data Breach Litigation

Cyber Law and Data Protection Alert | September 21, 2016
By: Joshua A. Mooney


The most obvious implication will be the resulting increase in litigation. Yet, here is a bigger problem: the Sixth Circuit based its determination that standing existed to sue a breach victim on actions it undertakes to mitigate damage and help consumers prevent the very harm that plaintiffs later sued over.

The facts of *Galaria* are straightforward. The breach victim, Nationwide, maintained records containing personal information of customers and potential customers, including names, dates of birth, marital statuses, employers, Social Security numbers, and driver's license numbers. On October 3, 2012, hackers breached Nationwide’s computer network and stole the personal information of 1.1 million people. *Id.* at *3.* In the underlying data breach litigation that followed, putative class actions alleged violation of the Fair Credit Reporting Act (“FCRA”) through Nationwide’s failure to adopt required procedures to protect against wrongful dissemination of plaintiffs’ data. Plaintiffs also alleged claims for negligence and invasion of privacy by public disclosure of private facts – all based on Nationwide’s failure to secure Plaintiffs’ data. *Id.* at *4.*

In support of their claims, plaintiffs alleged that an illicit international market exists for stolen personal data. According to the complaints, Nationwide’s data breach created an “imminent, immediate and continuing increased risk” that plaintiffs would be subject to identity theft. They cited a study purporting to show that in 2011 recipients of data-breach notifications were 9.6 times more likely to experience identity fraud and had a fraud incidence rate of 19%. They also alleged that victims of identity theft “typically spend hundreds of hours in personal time and hundreds of dollars in personal funds,” incurring an average of $354 in out-of-pocket expenses and $1,513 in total economic loss. *Id.* at *5.*

The federal district court dismissed the lawsuits, concluding that plaintiffs lacked statutory standing for the FCRA claims and lacked Article III standing for the negligence and bailment claims. The court also concluded that while plaintiffs had standing for their invasion of privacy claims, such claims failed to allege a cognizable injury. Plaintiffs appealed the trial court’s order, except for the dismissal of the invasion of privacy claims. *Id.* at *6-7.* The Sixth Circuit reversed.
In order to bring a lawsuit, a plaintiff must have standing under Article III of the United States Constitution; “[t]he doctrine of standing gives meaning to these constitutional limits by ‘identify[ing] those disputes which are appropriately resolved through the judicial process.’” Id. at *8 (citation omitted). In *Spokeo v. Robins*, 136 S. Ct. 1540, 1547 (2016), the United States Supreme Court explained that “the ‘irreducible constitutional minimum’ of standing consists of three elements.” Those elements are that 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." *Spokeo*, 136 S. Ct. at 1547; *Galaria*, 2016 U.S. App. LEXIS 16840 at *8. Focusing on the first two elements, the Sixth Circuit in *Galaria* concluded that plaintiffs met their burden of proof and established Article III standing at the pleading stage to survive a motion to dismiss. As litigators know, that is half the battle.

The *Galaria* court explained that”[t]o establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’ " *Galaria*, 2016 U.S. App. LEXIS 16840 at *8 (quoting *Spokeo*, at 1548). Where a plaintiff seeks to establish standing based on an imminent injury, "that 'threatened injury must be certainly impending to constitute injury in fact’”; “'[a] llegations of possible future injury' are not sufficient.” Id. at *9 (quoting *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013)).

The Sixth Circuit concluded that plaintiffs’ allegations of increased risk of identity theft, coupled with “reasonably incurred mitigation costs,” established a concrete and particularized imminent injury for purposes of standing. Critically, the court based its decision on the fact that (1) there was proof that the plaintiffs’ information was in fact stolen, (2) hackers had targeted it, and (3) Nationwide had offered free credit monitoring services to help consumers mitigate their danger:

There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. *Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year.* Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims’ data for the fraudulent purposes alleged in Plaintiffs’ complaints. [Bold added.]

Id. at *9-10.

That plaintiffs also could identify specific costs incurred by them from steps recommended by Nationwide in its data breach notification letter further supported the court’s finding that the underlying complaints alleged an imminent injury:

Although Nationwide offered to provide some of these services for a limited time, Plaintiffs allege that the risk is continuing, and that *they have also incurred costs to obtain protections—namely, credit freezes—that Nationwide recommended but did not cover.* This is not a case where Plaintiffs seek to "manufacture standing by incurring costs in anticipation of non-imminent harm.” [Citing *Clapper*, at 1155.] Rather, these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing. [Bold added.]

Id. at *10-11.
Under the second element, the Sixth Circuit in *Galaria* held that the alleged harm was “fairly traceable” to Nationwide’s alleged conduct so as to satisfy Article III standing. *Id.* at *13. To satisfy the “fairly traceable” element, a plaintiff need not allege proximate causation. “Indirect” injury is sufficient. *Id.* at *14. Here, the *Galaria* court held that plaintiffs had sufficiently alleged that their injuries were “fairly traceable” to Nationwide’s conduct, because Nationwide's alleged negligence allowed the breach to happen:

> Although hackers are the direct cause of Plaintiffs’ injuries, **the hackers were able to access Plaintiffs’ data only because Nationwide allegedly failed to secure the sensitive personal information entrusted to its custody.**

In other words, but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data. These allegations meet the threshold for Article III traceability, which requires "more than speculative but less than but-for" causation. [Bold added.]

*Id.* at *15.

Finally, the Sixth Circuit concluded that plaintiffs had statutory standing to bring their FCRA claims and therefore there was no need to evaluate the causes of action alleged in the complaints themselves. *Id.* at *17-18.

This decision goes beyond the lowering of the standing threshold. It also demonstrates why a data breach victim needs a cyber law attorney to help it navigate the inevitable legal minefield that will follow a data breach. For instance, when a company suffers a data breach, state notification statutes require those companies to notify persons whose information has been compromised. Many state laws actually will require that notification letters include information explaining to consumers what steps may be taken to mitigate or monitor against any potential harm. Connecticut law requires that credit monitoring services be offered. Many companies offer credit monitoring services as an act of goodwill.

Yet, in *Galaria*, the Sixth Circuit used the content of a breach victim’s notification letter and offer of credit monitoring services to permit multiple lawsuits to proceed against it. Does that leave a breach victim with an untenable, Hobson’s choice: comply with state notification laws and get sued, or potentially violate those laws to avoid creating Article III standing for future class actions? Is the message of “darned if you do” one that courts want to establish? Another concern is whether decisions like *Galaria* will create an adverse impact on response efforts undertaken by breach victims.

These are issues that breach victims are going to need to address when first responding to a breach and yet another reason why it is prudent to have cyber counsel help guide the response as early as possible when a breach has occurred.

For additional information, contact Josh Mooney (215.864.6345; mooneyj@whiteandwilliams.com) or another member of the Cyber Law and Data Protection Group.

*This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult a lawyer concerning your own situation and legal questions.*