Recent Circuit Court Opinions Offer Guidance on Challenging the Standing Requirement for Plaintiffs in Data Breach Cases

By following trends and monitoring successful defenses in data breach litigation, companies can often avoid the reputational harm caused by making headlines. For most companies, it is not a question of whether they have been breached; they have. Rather, the more salient inquiry is when the breach is discovered, what steps and actions those companies will take after the discovery.

A frequent response after learning a data breach has occurred is "what is our exposure?" That is not a simple question to answer—primarily because the law surrounding who has standing to sue is unsettled.[1] This is true for plaintiffs who seek to sue alone or as members of a class action. Individuals who can demonstrate actual use of their stolen data clearly have a better chance of meeting standing requirements based upon actual harm, but that does not mean that "use" is the threshold element. Actual use is in fact rare. Far more commonly, plaintiffs in data breach cases allege threatened or potential harm that may result from a data breach. Courts have struggled in such cases to draw the line between plausible harm sufficient to establish standing, and harm that is too speculative to satisfy Article III.

Recent court decisions, however, are helping to draw the lines of what plaintiffs must show to determine whether standing exists, and strategies that companies may employ to defeat claims of standing. These cases help guide companies and their counsel on answering the question of "what is our exposure?" In particular, two circuit courts recently issued important opinions on data breach standing in the last two months. While the Fourth Circuit's decision in *Beck v. McDonald*, et. al., No. 15-1395 may appear to conflict with the Third Circuit decision in *In re Horizon Healthcare Services, Inc.* issued just weeks earlier, the two are reconcilable.

In *Beck v. McDonald*, the Fourth Circuit affirmed the district court's dismissal on the basis that the plaintiffs failed to establish a non-speculative, imminent injury-in-fact as required for Article III standing. *Beck* arose from a laptop containing personal information being stolen and four boxes with pathology reports going missing. The plaintiffs claimed that they suffered harm including the increased risk of future identify theft and the cost of measures to protect themselves. The district court dismissed Beck's negligence claims at the pleading stage, but allowed the Privacy Act and the Administrative Procedure Act claims to go forward. McDonald moved for summary judgment. Here, time helped the defendant. Two years after the alleged breach and with the benefit of discovery, the plaintiffs could not show that the information on the laptop had been misused or accessed. Citing *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147-48, 1151 (2013), the Fourth Circuit explained that "threatened injury must be certainly impending to constitute injury in fact," and a plaintiff may not "manufacture standing merely inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Beck*, at 13, 14. The Fourth Circuit held that plaintiffs needed to show that "the thieves targeted the stolen items for the personal information they contained … the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities." Here, the court relied upon the passage of time without tangible injury to dismiss the plaintiffs' claims.

On the issue of whether there was an increased risk of future identify theft—a common claim in data breach cases—the Fourth Circuit acknowledged that there was a circuit split concerning whether this risk constituted an

injury-in-fact. The Sixth, Seventh and Ninth Circuits confer standing, at the pleading stage, when there is a threatened injury.[2] The First and Third Circuits require more.[3] In attempting to reconcile the split, the Fourth Circuit found that the Sixth, Seventh and Ninth Circuits' decisions actually supported the dismissal of the plaintiffs' claims in the case at hand as "too speculative" because, in those decisions, the plaintiffs had alleged that the data thief had intentionally targeted the personal information compromised in the data breaches. *See Id.*, at 18. However, after two years and extensive discovery, the *Beck* plaintiffs could not establish that their information had been accessed or misused in any way. *See Id.*, at 19.

Strategically, *Beck* supports the defense litigation decision to focus on whether information has been misused and allowing time for discovery when the defense does not believe that a plaintiff can demonstrate an actual injury. Here, the court found two years a sufficient metric. *Beck* further provides ammunition to the defense when plaintiffs fail to sue immediately following a breach, but still cannot demonstrate actual, as opposed to potential, harm. Finally, post-*Beck*, companies should continue to pursue standing arguments even if they are unsuccessful at the motion to dismiss stage, with a focus during discovery and dispositive motions on whether the plaintiffs' concerns about potential harm are too speculative.

Just days before the *Beck* decision, the Third Circuit conferred standing in another data breach litigation, *In re Horizon Healthcare Services, Inc.* In *Horizon*, the plaintiffs brought their claims under the Federal Credit Reporting Action (FCRA) alleging that Horizon, a consumer agency, acted willfully and negligently in failing to adequately protect their information and made "disclosures" when laptops were stolen. The district court dismissed plaintiffs' complaint for lack of standing, but the Third Circuit reversed. The Third Circuit held that the plaintiffs' allegations were sufficient to create a *de facto* injury even without evidence that the personal information was used improperly. The court recognized "there are some circumstances where the mere technical violation of a procedural requirement of a statute cannot, in and of itself, constitute an injury in fact." Citing *Spokeo, Inc. v. Robins* at 136 S. Ct. 1540, 1549 (2016) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."). The Third Circuit declined to define those limiting circumstances in *Horizon* and found that violation of the FCRA was sufficient to meet the concrete injury prong for standing, even without economic or tangible harm because the law was designed to protect the plaintiffs' personal information. While this case may seem in contrast to *Beck*, it can be distinguished based upon the nature of the underlying statute. In *Horizon*, the statute at issue was the FCRA. In *Beck*, the statutory schemes were the Privacy Act and Administrative Procedures Act. There is no mention of time in the *Horizon* decision. Presumably that is because the alleged violation of the FCRA itself was sufficient enough to provide a concrete injury that discovery into whether there had been any actual use of the information was unnecessary. Post-*Horizon*, companies defending FCRA litigation may have a more difficult time dismissing data breach cases for lack of standing than if the actions are brought under other statutes.

The same date as the *Horizon* opinion was released, the Seventh Circuit released its opinion in *Gubala v. Time Warner Cable* ---F.3d---, 2017. In *Gubala*, the court found that the plaintiff's contention that Time Warner Cable failed to destroy personal information belonging to him after he cancelled his subscription in violation of a statute did not create a plausible "concrete" risk of substantial harm because there was no accusation that the information had been made public. *Id.* at 2. While this case is not a "data breach" case, *Gubala* illustrates how courts are focusing the standing analysis on whether there is evidence that personal information has been used. Additionally,

it should be noted that in the time period at issue in the complaint, there was no evidence that the information had been made public or that it was being misused. Violation of the statute alone was insufficient. Companies need to proactively look at the statutes that cover them, and the law of the circuit in which they have been or are likely to be sued, and evaluate the risks.

Finally, the Eighth Circuit recently set aside a class settlement in the Target Corp. data breach litigation. *In re Target Corp. Customer Data Security Breach Litig. No. 16-3903*, 2017 WL 429621 (8th Cir. Feb. 1, 2017). Target had agreed to establish a $10 million settlement fund that would be allocated to class members with documented losses and then to members with asserted, but undocumented loss. Members who had not suffered any loss from the security breach would be bound by the release, but not receive any money from the fund. An objector to the settlement asserted that there was an intraclass conflict between those who either had suffered harm and those who might, but would have to release their claims. The Eighth Circuit instructed the district court to consider: (1) "whether an intraclass conflict exists when class members who cannot claim money from a settlement fund are represented by class members who can"; (2) "if there is a conflict, whether it prevents the class representatives from fairly and adequately protecting the interests of all of the class members"; and (3) "if the class is conflicted, whether the conflict is 'fundamental' and requires certification of one or more subclasses with independent representation." *Id.* at *3. While not framed as a standing issue, the Eighth Circuit's order grapples with the issue of how a court determines there is an injury and how it should be compensated.

The decisions in these different circuits all reflect the difficulties that courts are having in interpreting the U.S. Supreme Court's *Spokeo Inv. v. Robins* decision as it relates to standing in data privacy cases. Familiarizing oneself with the decisions and the individual facts at issue in each of them will help companies and their counsel address potential for exposure. Companies need to consider the statutes that apply to them, and establish appropriate safeguards in the forms of data policies and regular audits. Incident response plans should be crafted according to the particular situations of each company and draft notification letters and response team action items need to be in place ahead of time. Once a company has been accused of a data breach, the incident response plan should be put into immediate action, which includes careful examination of the relevant statutes that form the basis of the threats, and the potential forums in which they may be sued that will guide the exposure risk analysis. Knowing the trends of how those statutes are being applied in different jurisdictions is of paramount importance. From there, the strategy of examining the timing of when the alleged harm comes should take precedent. Moreover, as seen in the *Beck* case, if plaintiffs survive the challenges to the pleading, companies should continue to focus on standing issues throughout discovery, as the passage of time may strengthen the speculative nature of the harm asserted. Of course, many steps are involved in assessing, analyzing, and addressing data breaches, but if companies are up-to-date on the ever-evolving landscape of standing, they will be in a better position to evaluate and assess the exposure risks they face.

Jonathan C. Sandler
Shareholder
jsandler@bhfs.com
310.564.8672

Evan M. Rothstein
Shareholder
erothstein@bhfs.com
303.223.1116

Richard B. Benenson
Shareholder
rbenenson@bhfs.com
303.223.1203

Kerry J. LeMonte
Associate
klemonte@bhfs.com
303.223.1244

[1] "To 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.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). In *Spokeo*, the Supreme Court suggested that some violations of the Fair Credit Reporting Act ("FCRA"), though "intangible" harms, may still be sufficiently "concrete" to establish an Article III injury-in-fact. 136 S. Ct. at 1549–50.

[2] See *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016) (plaintiff-customers' increased risk of future identity theft theory established injury-in-fact after hackers breached Nationwide Mutual Insurance Company's computer network and stole their sensitive personal information, because "[t]here 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"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694–95 (7th Cir. 2015) (plaintiff-customers' increased risk of future fraudulent charges and identity theft theory established "certainly impending" injury-in-fact and "substantial risk of harm" after hackers attacked Neiman Marcus with malware to steal credit card numbers, because "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010) (plaintiff-employees' increased risk of future identity theft theory a "credible threat of harm" for Article III purposes after theft of a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 Starbucks employees); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 632–34 (7th Cir. 2007) (banking services applicants' increased risk of harm theory satisfied Article III injury-in-fact requirement after "sophisticated, intentional and malicious" security breach of bank website compromised their information).

[3] See *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (brokerage account-holder's increased risk of unauthorized access and identity theft theory insufficient to constitute "actual or impending injury" after defendant failed to properly maintain an electronic platform containing her account information, because plaintiff failed to "identify any incident in which her data has ever been accessed by an unauthorized person"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (plaintiff-employees' increased risk of identity theft theory too hypothetical and speculative to establish "certainly impending" injury-in-fact after unknown hacker penetrated payroll system firewall, because it was "not known whether the hacker read, copied, or understood" the system's information and no evidence suggested past or future misuse of employee data or that the "intrusion was intentional or malicious").