Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

8th Circ. Puts Down Standing Marker With Data Breach Rulings

By **Allison Grande**

Law360, New York (September 13, 2017, 9:13 PM EDT) -- The Eighth Circuit recently added to the increasingly fractured standing landscape that has emerged post-Spokeo by issuing a pair of decisions in putative data breach class actions that attorneys say demonstrate the court's skepticism toward harm that has yet to materialize and the challenges that plaintiffs are likely to face if they get past standing.

In the span of less than two weeks late last month, a separate pair of Eighth Circuit panels weighed in on lower courts' decision to nix on standing grounds consumer suits brought in the wake of data breaches at Scottrade and SuperValu — and reached somewhat disparate results. The Scottrade panel **found that the plaintiff's allegation** that he had paid for data security protections he never received was sufficient for standing, while the judges deciding the SuperValu case **concluded that the threat** of future identity theft from the breach was not enough of an injury to give standing to consumers who hadn't experienced credit card fraud.

"Through these decisions, the Eighth Circuit cemented its data breach standing principles in unusually clear terms," Benesch Friedlander Coplan & Aronoff LLP partner David Almeida said. "In the Eighth Circuit, where there is a contract or actual identity theft or credit card fraud, there will be standing."

Attorneys say that the decisions are significant not only for what they say about how the Eighth Circuit will approach the question of what type of harm will be sufficient to meet the standing bar established by the U.S. Supreme Court in Spokeo v. Robins, which held that a concrete injury is necessary for standing, but also for how much weight the court will give in the future to the type of data that has been breached and the growing efforts by the plaintiffs bar to allege overpayment for data security services.

The decisions also highlight that for plaintiffs, a victory on standing does not necessarily portend future success, according to attorneys.

"At the end of the day, the most important takeaway is that the Article III standing is simply a battle in data breach actions — it is far from the war," Almeida said.

Since the Supreme Court handed down its Spokeo decision in May 2016, courts across the country have grappled with how to apply the concrete injury standard to data breach

disputes, with mixed results.

"These two decisions from the Eighth Circuit illustrate the continued divergence of opinions regarding Article III standing for data breach claims," Troutman Sanders LLP partner David Anthony said.

In the SuperValu case, which was decided on Aug. 30, the Eighth Circuit was tasked with deciding if the allegation that credit card data was stolen but not misused was enough for standing.

Appellate courts both before and after the Spokeo ruling have been somewhat sympathetic to these claims. For example, the Seventh Circuit in a pair of pre-Spokeo decisions in disputes over data breaches at Neiman Marcus and P.F. Chang's found that the exposure of consumers' data was enough for standing. The Neiman Marcus court observed that the only reason that hackers would break into a store's database and steal consumers' private information was to misuse that data at some point.

And in **an Aug. 1 decision**, the D.C. Circuit joined at least five other circuits, including the Seventh, with its conclusion that a group of CareFirst policyholders had "cleared the low bar to establish their standing at the pleading stage" by asserting that there was a substantial risk that their stolen personal information could be used for purposes such as identity theft or medical harm even though it had yet to be misused.

However, the Eighth Circuit broke from these circuits in its SuperValu ruling, hewing more closely to the Second and Fourth Circuits by holding that "although others have ruled that a complaint could plausibly plead that the theft of a plaintiff's personal or financial information creates a substantial risk that they will suffer identity theft sufficient to constitute a threatened injury in fact, we conclude that plaintiffs have not done so here."

In upholding the dismissal of the claims brought by the 15 shoppers who couldn't prove that their payment cards had incurred fraudulent charges, the Eighth Circuit rejected the plaintiffs' reliance on a 2007 report from the Government Accountability Office to support their claims that the data breaches, which affected about 200 stores, had put them at an increased risk of identify theft. This holding likely will prove beneficial to companies fighting such cases, attorneys noted.

"This is significant because most data breach actions rely heavily on irrelevant and often decade-old studies to convince a court that there is a risk of possible identity theft," Almeida said.

While the Eighth Circuit's ruling is difficult to reconcile with standing decisions such as those that have come out of the Seventh Circuit, which also involved the compromise of credit card information, attorneys noted that the CareFirst decision out of the D.C. Circuit involved other sensitive personal information, such as names and subscriber ID numbers, a distinction that could play a role in such standing disputes moving forward.

"What we're seeing in this Eighth Circuit decision is a real drilling down into data elements," said Ed McAndrew, the co-practice leader of Ballard Spahr LLP's privacy and data security group. "While a stolen credit card number can be used to attempt to engage in fraudulent purchases once and then that card is shut down by the bank, the greater concern lies in information like Social Security numbers and driver's license numbers, which

can be used to open new accounts and alter credit history."

Thomas Zych, chairman of Thompson Hine LLP's emerging technologies practice, agreed that the nature of the stolen data "will and definitely should" be part of the calculus when it comes to standing and that he expected the **recent massive data breach** at Equifax that compromised 143 million consumers' personal data, including Social Security numbers, to now be "the elephant in the room" for courts weighing these kinds of cases.

"Courts inform themselves from the real world, and when they see a data breach of that kind and see Equifax tell consumers to go out and take precautions and expend time and money to do so, it's going to seem more plausible to the court that something bad has happened and that consumers have to take steps to protect themselves," Zych said.

Aside from departing from several circuits in its risk of future harm analysis, the Eighth Circuit also signaled a more measured approach to the standing issue by being willing to resurrect the suit with respect to one named plaintiff who had alleged that his credit card had been fraudulently charged, according to attorneys.

"Here, the Eighth Circuit is conducting a more nuanced standing analysis that requires going plaintiff by plaintiff and finding that only plaintiffs who had actually alleged unauthorized credit card charges had standing, and that fear of future misuse of card information is not enough," Carlton Fields shareholder Kristin Ann Shepard said.

While the approach worked in the plaintiffs' favor at the pleading stage, attorneys noted that this individualized analysis may not serve them quite as well during class certification.

"The implication of the ruling is that it limits the class to only those who allege fraudulent charges, which is likely to mean there will be a much smaller class and smaller exposure because most customers whose information is compromised never experience fraudulent charges," Shepard said.

And even if a class is able to be put together that contains only shoppers who incurred unauthorized charges, uncertainties about whether the misuse resulted from the SuperValu breach or some other data security incident will likely make certification even more difficult, especially given the standard established by the Supreme Court's 2011 decision in Wal-Mart v. Dukes that plaintiffs must share not only the same questions but also common answers in order to certify a class, attorneys noted.

"The question for all class members is going to be the same, namely: Did the breach cause fraudulent charges?" Shepard said. "But the answer is going to be different for each plaintiff because one might have gotten his information stolen from another data breach while another may have given his card to a waiter who misused it."

The Eighth Circuit provided similar guideposts to both sides of the bar in deciding the Scottrade case. The suit hinged on plaintiff Matthew Kuhns' claim that he had standing for his contract-related claims because the difference between the amount he paid to help Scottrade meet its contractual obligations to provide data management and security to protect his personally identifiable information and the value of the services he received — which purportedly did not include these security measures — was an actual economic injury.

Plaintiffs have increasingly been using this overpayment theory, which has long been used in other areas of the law, in an attempt to get in the door when it comes to privacy claims. The Eighth Circuit's endorsement of the strategy to establish standing in its Aug. 21 decision gives a boost to these efforts.

"If someone is able to say with a straight face that they would have paid $2 for an insecure service but instead they paid $3, I think courts will scrutinize those types of price differential claims," Zych said.

For companies, a takeaway from the Scottrade standing ruling is that what's said in privacy and data security policies matters and that they should make sure they are adhering to those statements, Shepard noted.

"If you make representations about privacy or data security of information collected in connection with a consumer contract, be prepared to deliver," Shepard said.

But at the same time, while the Eighth Circuit found standing, it ultimately ended up dismissing the suit due to Kuhns' failure to plausibly allege a breach of contract because there was no evidence that Scottrade misrepresented its security promises, and Kuhns didn’t identify any specifics to back up his contract claims.

"While the court didn't close the door on such claims entirely, it is saying that that the mere fact that a hacker was able to get your information is not enough to show a failure to comply with a privacy policy. You have to have something specific," Shepard said.

In light of the Eighth Circuit rulings, attorneys expect plaintiffs to shift their focus to circuits that give more weight to injuries that have yet to come to fruition and for defendants to continue to focus on steps beyond standing where an escape is likely to be easier.

"Following the Supreme Court’s decision in Spokeo, these Eighth Circuit opinions help to confirm that standing requires a 'concrete injury' or one that is 'real and not abstract,'" Anthony said. "Not surprisingly, courts will continue to struggle with these distinctions, and plaintiffs counsel will continue their efforts to establish Article III standing for data breach claims."

The Scottrade customer is represented by Joseph J. Siprut, Richard L. Miller II and Richard S. Wilson of Siprut PC, Timothy G. Blood, Thomas J. O’Reardon II and Paula R. Brown of Blood Hurst & O'Reardon LLP, and John G. Simon and Anthony G. Simon of The Simon Law Firm.

Scottrade is represented in the district court by Brandi Lynne Burke, Christopher M. Hohn, David M. Mangian and Thomas E. Douglass of Thompson Coburn LLP.

The SuperValu shoppers are represented by Ben Barnow of Barnow & Associates PC, Edwin Kilpela Jr. of Carlson Lynch Sweet Kilpela & Carpenter LLP, Rhett McSweeney and David Langevin of McSweeney/Langevin LLC, Karen Riebel of Lockridge Grindal Nauen PLLP, Aron Robinson of Law Office of Aron D. Robinson, John Driscoll and Christopher Quinn of The Driscoll Firm PC, Richard Coffman of The Coffman Law Firm, and John Steward of Steward Law Firm LLC.

SuperValu is represented by Harvey Wolkoff, David Cohen and Kathryn E. Wilhelm of Ropes

& Gray LLP and Stephen Safranski of Robins Kaplan LLP. Albertsons is represented by John Landolfi and Christopher Ingram of Vorys Sater Seymour & Pease LLP and Marc Al of Stoel Rives LLP.

The cases are Kuhns v. Scottrade Inc., case numbers 16-3426 and 16-3542, and Melissa Alleruzzo et al. v. SuperValu Inc. et al., case number 16-2528, in the U.S. Court of Appeals for the Eighth Circuit.

--Editing by Christine Chun and Breda Lund.
