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

DC Circ. Piles Onto Standing Split With Data Breach Ruling

By **Allison Grande**

Law360 (June 28, 2019, 5:32 PM EDT) -- Circuit courts are continuing to reach divergent conclusions over whether the threat of data misuse is enough to allow data breach litigation to move forward, highlighting the growing need for the U.S. Supreme Court to bridge the gap.

In a recent ruling reviving litigation over a data breach at the U.S. Office of Personnel Management, the D.C. Circuit split with several sister circuits in concluding that the heightened risk of identity theft was enough to clear the "low bar" for establishing standing at the pleading stage.

Even though evidence of widespread identity theft and financial fraud has yet to emerge, the panel in a 52-page per curiam ruling found that the plaintiffs had plausibly alleged the sophisticated nation-state hackers believed to be behind the 2015 hack could still use the sensitive pilfered data for these nefarious purposes.

"This decision furthers the importance for one of these cases on standing to get to the Supreme Court for resolution of this circuit split because right now, so much of the viability of consumer class actions in the data breach context depends on what circuit the case is being heard in, and that issue will need to get resolved in the upcoming years," said April Doss, a partner at Saul Ewing Arnstein & Lehr LLP.

The June 21 ruling in the OPM dispute is consistent with the D.C. Circuit's August 2017 decision in similar litigation over a data breach at CareFirst. In that case, which the Supreme Court declined to take up last year, the appellate panel held that the CareFirst policyholders had “cleared the low bar to establish their standing at the pleading stage” by asserting there was a substantial risk that their stolen personal information could be used “for ill" purposes, such as identity theft, even though it had yet to be misused.

The OPM ruling strengthened that holding while delving even deeper into issues such as whether the hackers' identity and apparent motivations should play any role in determining the potential for future harm and whether plaintiffs could ever plausibly link an instance of identity theft or fraud to one of the scores of hacks that are increasingly coming to light.

Electronic Privacy Information Center President Marc Rotenberg, whose group filed an amicus brief in support of the plaintiffs in the OPM case, called the D.C. Circuit's standing analysis "clear and compelling."

"The close association between data breach and identity theft is well established," Rotenberg told Law360. "The court put it well: 'It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft.'"

But not all appellate courts have agreed with this assessment. While the Sixth, Seventh and Ninth circuits have allowed data breach litigants to proceed based on the alleged heightened risk of future misuse, several appellate courts — the Second, Third, Fourth and Eighth — have imposed a heightened standard that requires some actual harm to have already manifested.

The D.C. Circuit in its latest opinion distinguished two of these conflicting results — the Fourth Circuit's 2017 ruling in Beck v. McDonald and the Third Circuit's 2011 ruling in Reilly v. Ceridian Corp.

The Fourth Circuit held in the Beck case that the risk of future identity theft stemming from the theft of a laptop and boxes of medical records was too speculative because the plaintiffs had failed to allege the thief "intentionally targeted" the stolen information or had used it to commit identity theft. The Third Circuit in the Reilly case refused to find standing due to a lack of evidence the hacker had ever read, copied or understood the payroll data that was potentially accessed.

The OPM breach case was different, the D.C. Circuit panel ruled, because the plaintiffs alleged the hackers had intentionally targeted the compromised data and misused that information, which were "precisely the types of allegations missing" from the contradictory cases.

"What was really working in favor of the plaintiffs in the OPM case was that they were able to allege that certain identity theft had already occurred, and the court really rejected the district court's thinking in terms of the possibility that those instances of fraud and identity theft could have been caused by other thefts of information," said Tucker Ellis LLP counsel Avril Love.

The panel's decision to push back at these contrary rulings and extend its Attias v. CareFirst ruling to government agency breaches "preserves the prior circuit split scorecard and really underscores the desirability of the Supreme Court ultimately weighing in on the issue," said Orrick Herrington & Sutcliffe LLP partner Michelle Visser.

"Overall, the issue of standing in privacy and cyber cases is something that litigants and courts are still grappling with and looking for clear answers that currently don't exist," Visser said.

The high court has tackled the issue of standing before, most notably in a pair of recent major privacy decisions.

In Clapper v. Amnesty International, the justices ruled in 2013 that injuries must be real or imminent and not merely speculative. The Supreme Court followed that with its 2016 decision in Spokeo v. Robins, which held that harm must be concrete and mere statutory violations do not suffice.

But while these cases shed some light on the requirements for establishing standing, they've left unresolved the vital questions of what data breach harms are concrete and imminent enough to meet these standards and whether plaintiffs can actually establish a direct link between the injuries they've suffered and a specific data breach.

"Those Supreme Court decisions were both well reasoned and nuanced, but there isn't yet a bright-line rule where data breach plaintiffs will always have a claim here but not there," said Axinn Veltrop &

Harkrider LLP partner Thomas Rohback. "Things are still in flux, and the real trick will be for someone at some point to figure out where the damage is."

The Supreme Court has already declined to consider the widening standing split when pressed in both the CareFirst case and in data breach litigation against shoe retailer Zappos, which yielded a Ninth Circuit ruling that the risk of future harm from the theft of consumer data is enough for standing.

It's unclear whether the OPM and its contractor KeyPoint Government Solutions will appeal the D.C. Circuit's decision to the high court. Neither party responded to a request for comment on the ruling.

Jordan Elias of Girard Gibbs LLP, counsel for the plaintiffs' group that includes the American Federation of Government Employees and 38 individuals, indicated in a recent email this his side was ready to move on from the standing question.

"We are pleased with the ruling and look forward to returning to the trial court to pursue relief on behalf of the millions of victims of this data breach," Elias told Law360.

The government employees are pursuing a Privacy Act claim, which the D.C. Circuit declined to dismiss after rejecting the argument that sovereign immunity barred the allegation.

If the standing debate does continue, significant ink is likely to be spilled over the issue of causation, which fueled a notable partial dissent by D.C. Circuit Judge Stephen F. Williams.

While his colleagues found it highly probable that the hackers were motivated at least partially by financial gain and faulted the lower court for relying on the suggestion that the Chinese government was behind the attack, Judge Williams embraced a different view of the attack, which compromised Social Security numbers, addresses, fingerprint records and other sensitive information belonging to 21.5 million current, former and prospective government employees.

In his 17-page opinion dissenting in part, Judge Williams found that "the garden-variety identity theft theory" advanced by the government employee plaintiffs failed to make it over the line "from conceivable to plausible" in light of the "obvious alternative explanation" that the nation-state-backed hackers executed the cyberattack "for espionage or kindred purposes having nothing to do with identity theft."

The judge also expressed reservations with his colleagues' unwillingness to assume the risk of identity theft had passed. Instead, Judge Williams wrote that the "striking dearth of allegations as to any pattern of unusual or higher-than-ordinary identity theft or fraud" supported the conclusion that the hack was "focused entirely on pursuit of espionage and kindred threats to national security" and that further injury to the government workers was highly unlikely.

The panelists' dueling viewpoints drive home the difficulties with finding a uniform resolution to these thorny standing questions, attorneys say.

"Some courts are looking at breaches and assuming bad things are going to happen to people affected, and some are not willing to make that assumption," Mayer Brown LLP partner Stephen Lilley said. "As evidenced by the majority opinion and partial dissent in the OPM case, even judges who are looking at the same sets of allegations are viewing these issues differently."

For businesses that hold sensitive data, the D.C. Circuit case underscores that "their potential legal liability and legal risk is not necessarily going to be limited by who did the hacking," Doss added.

"Nobody should be expecting that the identity of the hacker or the reason behind the attack is going to be dispositive on whether there's harm to individuals," Doss said.

The D.C. Circuit's standing embrace is likely "to put wind in the sails of plaintiffs' lawyers handling privacy and data security cases," according to Casey Quinn, an attorney with Newmeyer & Dillion LLP's privacy and data security practice.

"This increases the likelihood that people whose data was breached will qualify to participate in a suit, which in turn should increase the desire of both government and private entities to protect data," Quinn said.

The D.C. Circuit's low standing bar and its staunch criticism of the OPM and KeyPoint's alleged data security failings additionally reflect shifting attitudes toward consumer privacy in the wake of developments such as the passage of the European Union's General Data Protection Regulation and California's landmark Consumer Privacy Act, Baker Botts LLP special counsel Cynthia Cole noted.

"The opinion goes into detail about how OPM should have known that its policies and security was lax and that, given the nature of the information they had, they should have been hyper-vigilant about protecting it, and that's the kind of language that looks a lot like something you'd see in the GDPR," Cole said.

The growing movement toward embracing "a less concrete version of harm that's measured not just by someone making fraudulent charges with a stolen credit card" may also spur Congress to finally enact a federal privacy law that would serve as "some kind of unifying legislation on the issue" and alleviate the need for courts to "step in and move the needle in ways that policymakers have yet to do," Cole added.

No matter how the standing divide shakes out, the laser focus on data security is unlikely to subside anytime soon.

The National Treasury Employees Union, which along with three individuals formed the second group of plaintiffs in the OPM case, drove home this point in responding to the ruling.

While the D.C. Circuit found standing for the union, the court highlighted the difficulties that plaintiffs face with keeping allegations afloat beyond the standing stage by concluding the group had failed to adequately plead its claim that the OPM's flawed information-storage measures violated their constitutional right to informational privacy.

The union's national president, Tony Reardon, said in a statement that while NTEU was disappointed with the dismissal of its constitutional claim, it appreciated the court's acknowledgment of "the severity and scope of OPM's data security shortcomings."

"NTEU has laid bare that OPM was aware of the critical weaknesses in its system and that it has done nothing meaningful to strengthen its safeguards," Reardon said. "We expect OPM to take every precaution available to protect the information it holds so no other federal employees are ever faced with an uncertain future because their personal information has been stolen."

Circuit Judges David S. Tatel, Patricia A. Millett and Stephen F. Williams sat on the panel for the D.C. Circuit.

The employees are represented by Peter A. Patterson and David H. Thompson of Cooper & Kirk PLLC, Daniel C. Girard and Jordan Elias of Girard Sharp LLP, Tina Wolfson of Ahdoot & Wolfson PC, Gary E. Mason of Whitfield Bryson & Mason LLP and Richard B. Rosenthal.

The National Treasury Employees Union is represented in-house by Paras N. Shah, Gregory O'Duden, Larry J. Adkins and Allison C. Giles.

The OPM is represented by Sonia M. Carson and Mark B. Stern of the U.S. Department of Justice.

KeyPoint is represented by Jason J. Mendro, F. Joseph Warin, Matthew S. Rozen and Jeremy M. Christiansen of Gibson Dunn & Crutcher LLP.

The case is In re: Office of Personnel Management Data Security Breach Litigation, case numbers 17-5217 and 17-5232, in the U.S. Court of Appeals for the District of Columbia Circuit.

--Editing by Philip Shea.