ALERT MEMORANDUM

With Equifax Looming, Split On Standing In Data Breach Cases Grows with Recent Decisions

October 4, 2017

As the Equifax breach litigation gets underway, several recent decisions have widened a split on when and under what conditions customers or other affected individuals may bring claims against a company that suffers a data breach. Late last month, a D.C. federal judge dismissed a lawsuit based on the massive breach at the U.S. Office of Personnel Management ("OPM"), ruling that the theft of data alone was not enough to establish standing. The Court of Appeals for the Eighth Circuit issued a similar recent ruling, holding that plaintiffs suing the grocery retail company SuperValu had not shown that they were at greater risk of identity theft as a result of a data breach at the company and they therefore lacked standing. In contrast to these decisions, a California federal judge allowed claims to proceed against Yahoo! based on the allegation that the customer-plaintiffs alleged a risk of future identity theft and loss of value of their personal identification information. The differing interpretations of the standing requirements in data breach cases will no doubt continue to be vigorously litigated and may ultimately need to be resolved by the Supreme Court.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

WASHINGTON
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1801
T: +1 202 974 1500
F: +1 202 974 1999

Tanner Mathison
+1 202 974 1548
tmathison@cgsh.com

Background: The Data Breaches

The recent decisions arise from three different data breaches at OPM, SuperValu, and Yahoo!:

— In June 2015, federal officials announced that OPM had been the target of a data breach targeting millions of people, including government employees and others. According to numerous reports, the attack originated in China and last month the FBI arrested a Chinese national connected to the malware used in the breach.

— In 2014, unknown computer hackers accessed SuperValu's payment processing systems and gained access to customer names and credit card information. SuperValu disclosed the breach shortly thereafter.

— Between 2013 and 2016, Yahoo! suffered three massive data breaches. Yahoo! originally disclosed the attacks in late 2016 and just yesterday announced that the breach was bigger than initially described, potentially affecting all 3 billion of its accounts.

As has become increasingly common, on the heels of the disclosure of each of these breaches, plaintiffs' law firms promptly brought claims on behalf of customers against the companies. The plaintiffs alleged violations of state consumer protection laws, breach of contract, and common law negligence and claimed that their heightened risk of identity theft, among other alleged injuries, was sufficient to establish standing.

In the recent cases involving OPM, SuperValu, and Yahoo!, one court agreed with plaintiffs that they had established standing, while the other two courts agreed with the defendants and dismissed the cases.

The Growing Split on Standing Requirements

The standing requirement under Article III of the U.S. Constitution limits federal court jurisdiction to actual cases and controversies. Under the Supreme Court's most recent standing decision, in a case called *Spokeo*, plaintiffs must allege a "concrete and particularized" injury that is "actual or imminent, not conjectural or hypothetical."[1] As was discussed in our prior alert memorandum, multiple circuits have held that exposure of consumers' data to potential identity theft is sufficient to establish Article III standing.[2] While at least two circuits have held the opposite.[3]

The OPM Decision. In the OPM litigation, the United States District Court for D.C. held that plaintiffs had not pled an actual injury beyond the mere theft of their data, which it found was insufficient to establish Article III standing.[4] The court distinguished the OPM breach from breaches of retail companies, which the court believed could support an inference that hackers obtained information to make fraudulent charges or commit identify theft.[5] The court found that such assumptions did not apply in the OPM breach context, which involved the theft of government employee information potentially by Chinese nationals. Even for the plaintiffs who did allege that they had already experienced an actual misuse of their credit card numbers or personal information, the court held that they could not tie those disparate incidents to the OPM breach. Accordingly, the court dismissed the case for lack of standing.

[1] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016)
[2] *See e.g.*, *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *1, *3 (6th Cir. Sept. 12, 2016); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).
[3] *See Whalen v. Michaels Stores, Inc.*, --- F.3d ---, 2017 WL 1556116 (2d Cir. May 2, 2017)*; Beck v. McDonald*, 848 F.3d 262, 268 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, No. 16-1328, 2017 WL 1740442 (U.S. June 26, 2017).
[4] *In re: U.S. Office of Personnel Management Data Security Breach Litigation*, Misc. Action No. 15-1394 (ABJ), MDL Docket No. 2664 (D.D.C. Sept. 19, 2017).
[5] The court distinguished *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017), where the D.C. Circuit held that plaintiffs had established standing based on claims that their information was stolen from a health insurance company. That decision is discussed in our prior alert memorandum available here.

The SuperValu Decision. In the SuperValu case, plaintiffs who had their credit card information stolen relied on a 2007 Report from the Government Accountability Office (the "2007 GAO Report") to support their "otherwise bare [standing] assertion that '[d]ata breaches facilitate identity theft.'"[6] The court reasoned that because the stolen credit card information could not be used to open new accounts, the only possible risk to the plaintiffs was credit card fraud. However, the 2007 GAO Report relied on by the plaintiffs also stated that "most breaches have *not* resulted in detected incidents of identity theft."[7] For these reasons, the Eighth Circuit held that the plaintiffs' allegations did "not plausibly support the contention that consumers affected by a data breach face a *substantial risk* of credit or debit card fraud," and thus did not establish standing under *Spokeo*. Nevertheless, in a footnote, the court stated, "[w]e recognize there may be other means—aside from relying on reports and studies—to allege a substantial risk of future injury, and we do not comment on the sufficiency of such potential methods here."[8]

The Yahoo! Decision. In contrast to these two decisions, the District Court for the North District of California allowed plaintiffs' claims to proceed against Yahoo! Among other things, the court held that the alleged "risk of future identity theft" and the loss of value of personal identifying information were sufficient injuries to justify the plaintiffs' standing to bring suit.[9] In doing so, the court relied on the Ninth Circuit's decision *In re Facebook Privacy Litigation*, 72 F. App'x 494, 494 (9th Cir. 2014), which found that the plaintiffs plausibly alleged that they experienced harm where the plaintiffs' personal information was disclosed in a data breach and they therefore "los[t] the sales value of th[eir] [personal] information." Thus, the *Yahoo!* and *Facebook* decisions are in tension with the two other recent decisions outside of the Ninth Circuit discussed above, which held that similar allegations did not establish Article III standing in those cases.

Takeaways

With a growing number of courts coming to different outcomes on the viability of data breach litigation, it is likely that these issues will continue to be at the forefront of breach litigation cases, including in the Equifax consumer cases. Data breach plaintiffs will likely seek to marshal as much factual support for their allegations of heightened risk of injury and, if they are able, actual injury caused by the breach. This will likely turn on the types of data compromised, the relationship between the victims of the breach and the data custodian (including any relevant contractual relationship or state laws governing the relationship), and what is known about the source of the breach, if anything. Ultimately, if courts continue to come to differing outcomes in factually analogous cases, the Supreme Court may choose to address the split and have the final word on the issue.

…

CLEARY GOTTLIEB

[6] *In re: SuperValu, Inc., Customer Data Security Breach Litigation*, 16-2378 Slip Op. at 10-11 (Aug. 30, 2017)
[7] 2007 GAO Report at 21 (emphasis added).
[8] *In re: SuperValu, Inc., Customer Data Security Breach Litigation*, 16-2378 Slip Op. at 10-11 (Aug. 30, 2017).
[9] In Re: Yahoo! Inc. Customer Data Security Breach Litigation, 16-MD-02752-LHK: 94 (Aug 30, 2017).