DEEPENING THE DIVIDE: D.C. CIRCUIT CONTINUES CIRCUIT SPLIT REGARDING STANDING IN DATA BREACH CLASS ACTION BASED ON RISK OF FUTURE HARM

Date: 9 July 2019

U.S. Consumer Financial Services and Class Action Litigation Defense Alert

By: Andrew C. Glass, Matthew N. Lowe

The D.C. Circuit Court of Appeals recently reaffirmed its position that a plaintiff can establish Article III standing (federal court subject matter jurisdiction) based solely on the risk of potential future harm following a data breach involving his or her personal information. The decision continues the split between the federal circuit courts of appeals regarding the issue.

In re Office of Personnel Management arose out of an alleged 2014 data breach of the eponymous office (the "OPM"). [1] The plaintiffs, current and former federal employees and their unions, sought to represent a putative class of individuals whose personal information, including social security numbers, addresses, and birth dates, was allegedly exposed in the breach. [2] The plaintiffs asserted that certain putative class members had experienced financial fraud or identity theft as a result of the breach and that other members faced the "ongoing risk that they … will become victims of financial fraud and identity theft in the future." [3] The district court ruled that the plaintiffs lacked standing to sue, holding that the putative class members who had allegedly experienced financial fraud had not pleaded facts demonstrating that the fraud was traceable to the OPM, and that the members who had only pleaded risk of future injury did not plausibly allege that such injury was either substantial or clearly impending. [4]

On appeal, the D.C. Circuit reversed, holding that the plaintiffs had adequately alleged standing based upon "the risk of future identity theft." [5] The court found that there was "no question that the OPM hackers … have in their possession all the information needed to steal … Plaintiffs' identities," citing as support the allegations that certain putative class members had already suffered actual identity theft. [6] And reaffirming its 2017 decision that it is a "low bar to establish … standing at the pleadings stage," the D.C. Circuit concluded that the plaintiffs had "plausibly alleged a substantial risk of future identity theft that is fairly traceable to OPM's … cybersecurity failings." [7]

Judge Stephen Williams concurred in part and dissented in part. Judge Williams noted that the breach is "more likely explained as the handiwork of foreign spies looking to harvest information about millions of federal workers for espionage" and thus that the complaint "d[oes] not plausibly suggest identity theft as the motive (and hence a source of future harm)." [8] Judge Williams also noted that the plaintiffs had failed to show any causation between the data breach and the actual identity theft that occurred for certain class members. [9] The majority, however, brushed aside these concerns, remarking that "espionage and identity theft are not mutually exclusive." [10] That some members suffered actual identity theft "suffices to support a reasonable inference that [the] Plaintiffs' risk of

future identify theft is traceable to the OPM cyberattacks." [11] The D.C. Circuit also distinguished two decisions from the Third and Fourth Circuits that fall on the other side of the split and generally reject standing based solely on an alleged risk of future harm flowing from a data breach. [12] The D.C. Circuit cited the Ninth Circuit in support its position. [13]

In re OPM is largely a re-affirmance of the D.C. Circuit's prior position that a plaintiff in a data breach litigation can establish standing at the pleading stage by alleging risk of future identity theft. But the decision deepens the divide between circuits such that the Supreme Court may take up the issue to resolve the conflict. For a summary of the circuit split and the various approaches taken by different circuits, please refer to our prior articles here and here as well as our articles summarizing recent decisions by the Seventh and Eighth Circuits here and here. We will continue to monitor and report on developments regarding data breach litigation in the D.C. Circuit and elsewhere.

NOTES

[1] *In re Office of Personnel Mgmt. Data Sec. Breach Litig.*, No. 17-5217, --- F.3d ---, 2019 WL 2552955, at *1 (D.C. Cir. Jun. 21, 2019) (*per curiam*).

[2] *Id.* at *1.

[3] *Id.* at *1, 6.

[4] *Id.* at *4.

[5] *Id.* at *5.

[6] *Id.* at *6 ("It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft.")

[7] *Id.* at *9-10 (citing *Attias v. Carefirst, Inc.*, 865 F.3d 620, 622, 629 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018)).

[8] *Id.* at * 22-23 (internal quotation marks omitted).

[9] *Id.* at *25. Judge Williams further explained that "3.3% of the population will experience some form of identity theft" each year so it is "not surprising" that a few plaintiffs in the 21.5 million member class would have suffered some identity theft, but this alone did not demonstrate causation. *Id.* "A handful of [the] Plaintiffs, for instance, almost certainly experienced a home invasion since the data breach [b]ut that doesn't imply a 'substantial risk' that *these hackers* have plans to break into the homes of [other class members]." *Id.* (emphasis in original).

[10] *Id.* at 6-7, 9.

[11] *Id.*

[12] *Id.* at *7 (distinguishing *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) and *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017)).

[13] *Id.* at *9 (citing *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019)).

KEY CONTACTS

ANDREW C. GLASS
PARTNER

BOSTON
+1.617.261.3107
ANDREW.GLASS@KLGATES.COM

