WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

District Court Confirms Data Breach Plaintiffs Must Demonstrate "Substantial Risk" of Future Harm to Establish Standing While Another Finds a Mere Statutory Violation Sufficiently Concrete to Confer Standing

August 17, 2016

AUTHORS

James C. Dugan | **Elizabeth J. Bower** | **Daniel K. Alvarez**

Two district court cases – decided the same day last week – highlight the unsettled state of standing in data breach cases.

District Court for the District of Columbia Requires "Substantial Risk" of Identity Theft

On August 10, 2016, the District Court for the District of Columbia joined the growing number of courts that have confirmed that data breach plaintiffs alleging only a risk of future identity theft face an exceptionally high bar to establish standing.

Attias v. CareFirst, Inc.[1] is one of three cases stemming from a breach of health insurer CareFirst's database that compromised the personal information of approximately 1.1 million policyholders. The information stolen included policyholders' names, birth dates, email addresses, and subscriber ID numbers, but not their social security or credit card numbers. The class plaintiffs in *Attias* alleged that this breach of their personal information compromised their identities and resulted in an increased risk of future identity theft. Judge Christopher Cooper dismissed the complaint for lack of

[1] *Attias v. CareFirst, Inc.*, Case No. 15-cv-00882 (CRC) (D.D.C. Aug. 10, 2016).

standing, however, and observed that the plaintiffs had failed to demonstrate the existence of a "substantial risk that stolen data has been or will be misused in a harmful manner."

Applying the standard provided by the U.S. Supreme Court in *Clapper v. Amnesty International*,[2] Judge Cooper assessed whether the risk of identity theft to the plaintiffs is "certainly impending" or "substantial." Though courts have diverged on which factors tend to indicate a "substantial risk" of harm to data breach plaintiffs, Judge Cooper cited two illustrative cases to guide his analysis: *In re Sci. Applications Int'l Corp.* ("*SAIC*")[3] and *Remijas v. Neiman Marcus Group*.[4] In *SAIC*, a case Judge Cooper considered somewhat similar to *Attias*, plaintiffs alleged an increased risk of future identity fraud caused by the theft of back-up tapes containing social security numbers from an individual's car. The *SAIC* court, however, found that the plaintiffs did not have standing because demonstrating the risk of harm required "too many assumptions . . . to find the alleged harm certainly impending." In *Remijas*, by contrast, a group of plaintiffs established standing based on the risk of future harm by demonstrating that 9,200 affected individuals had already suffered *actual* identity theft as a result of the intentional breach of Neiman Marcus's systems. In discussing these two examples, Judge Cooper seems to recognize that the determining factor for standing in data breach cases may often be the "series of assumptions required to find concrete harm."

The *Attias* plaintiffs argued that their case was similar to *Remijas* and that the intentional breach of CareFirst's server for the purpose of acquiring personal information weighed in favor of finding standing. Judge Cooper, however, distinguished *Remijas* in two significant ways. First, the *Attias* plaintiffs did not plausibly allege *any* individuals affected by the data breach had actually experienced identity theft or harm fairly traceable to the data breach. As both Judge Cooper and the *Chambliss* court found,[5] the lack of any individuals suffering actual identity theft from the CareFirst breach contrasts starkly with *Remijas*, in which the plaintiffs demonstrated a "substantial risk" of future harm by establishing that the Neiman Marcus hackers had "the means and the will" to misuse their personal information. Second, even if the hack was intentional, rather than coincidental, the type of personal information exposed in the CareFirst data breach was not of the type ordinarily used to commit identity theft. In other words, the plaintiffs failed to allege that the personal information exposed in the breach—names, birth dates, email addresses, and subscriber information—could or would be used to steal the plaintiffs' identities or to obtain *additional* personal information sufficient to steal their identities (*e.g.*, social security numbers). As the *SAIC* court observed, such facts require "too many assumptions" to find a "substantial risk" of identity theft sufficient to confer standing.

---

2 *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

3 *In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d 14 (D.D.C. 2014).

4 *Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688 (7th Cir. 2015).

5 *Chambliss* was the first of the three CareFirst cases to be addressed and was dismissed on similar grounds in May 2016. *Chambliss v. CareFirst, Inc.*, Case No. RDB-15-2288 (D. Md. May 27, 2016).

District Court Confirms Data Breach Plaintiffs Must Demonstrate "Substantial Risk" of Future Harm to Establish Standing While Another Finds a Mere Statutory Violation Sufficiently Concrete to Confer Standing

The *Attias* plaintiffs also alleged that violations of their rights under statutory consumer protection acts were sufficient to confer standing. Judge Cooper rejected this argument. Relying on the U.S. Supreme Court's recent decision in *Spokeo, Inc. v. Robins*,[6] which we wrote about in a recent client memorandum, Judge Cooper held that violations of statutory rights are insufficient to confer standing on a plaintiff who has not otherwise alleged concrete harm.

The District Court for the Southern District of Florida Finds Violation of Substantive Statutory Right to be Free From Heightened Risk of Identity Theft Sufficient to Confer Standing

The same day, however, the District Court for the Southern District of Florida interpreted *Spokeo* differently. In a case involving high-end retailer Jimmy Choo, Judge Beth Bloom held that a plaintiff established standing merely by alleging that she had been provided with a credit card receipt listing the card's expiration date—a purported violation of the Fair and Accurate Credit Transactions Act ("FACTA"). In *Wood v. J Choo USA, Inc.*,[7] the court held that "FACTA endows consumers with a legal right to protect their credit identities," so the plaintiffs "suffered a concrete harm as soon as Jimmy Choo printed the offending receipt." In doing so, Judge Bloom seized on *Spokeo*'s equivocation that violations of statutory rights can "[i]n some circumstances . . . be sufficient to constitute injury in fact" and found FACTA to be such a circumstance. *J Choo* follows another recent case in the Southern District of Florida, *Guarisma v. Microsoft*.[8] *Guarisma* distinguished the types of "procedural" rights cited in *Spokeo*—such as the right to notification by consumer reporting agencies of certain information—from those instances where "Congress has endowed plaintiffs with a *substantive* legal right" entitling plaintiffs to sue "without establishing additional harm." In other words, once a plaintiff establishes that a defendant violated a *substantive* right instead of a *procedural* right, the plaintiff has established that the harm is concrete.[9]

In light of continued uncertainty surrounding the level of harm data breach plaintiffs must allege to survive a motion to dismiss for lack of standing, companies must remain vigilant to protect personal information from the persistent threat of data breaches and compliant with statutory requirements designed to minimize the risk of and harm from identify theft and fraud.

---

6 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

7 *Wood v. J Choo USA, Inc.*, Case No. 15-cv-81487-BLOOM/Valle (S.D. Fla. Aug. 10, 2016).

8 *Guarisma v. Microsoft Corp.*, Case No. 15-24326-CIV-ALTONAGA/O'Sullivan (S.D. Fla. Jul. 26, 2016).

9 If *Guarisma* proves to be a helpful guide for future courts, plaintiffs are likely to focus on the legislative history underlying consumer protection statutes, as legislative "intent is particularly significant" to an analysis of whether a substantive legal right was intended. *Id.* at *4 n.2.

If you have any questions regarding this memorandum, please contact James C. Dugan (212-728-8654; jdugan@willkie.com), Elizabeth J. Bower (202-303-1252; ebower@willkie.com), Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com) or the Willkie attorney with whom you regularly work.

August 17, 2016