

Favorable Trend for Plaintiffs in Data Breach Class Actions: Circuits Differ on Whether Free Credit Monitoring Supports Standing

Enterprises responding to a data breach must be careful in crafting customer notifications and remedial measures, especially the provision of free credit monitoring services, due to these actions' potential impact on standing for class action plaintiffs. The 6th and 7th Circuits have found that post-breach mitigating actions like the provision of free credit monitoring services may constitute an admission of injury sufficient to give rise to standing. This trend, however, was criticized in the 3rd Circuit's recent opinion in *In Re Horizon Healthcare Services, Inc. Data Breach Litigation*, No. 15-2309 (3d Cir. 2017). Nonetheless, in this uncertain environment companies should be mindful of the potential impact of certain remedial measures on subsequent class actions.

Most federal privacy class action cases concern Article III standing as well as standing under the *Fair Credit and Reporting Act* (the "**FCRA**"). In its two most recent standing opinions, *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013) and *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), the Supreme Court raised the bar for Article III standing and statutory standing, respectively.

Both *Clapper* and *Spokeo* affirmed the basic three-part test required for standing first set out in the Supreme Court's decision in *Lujan v. Defs. of Wildlife*, 504 U.S. 555 (1992). To have standing, a plaintiff "must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." In *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), which predated *Clapper* and involved the theft of a laptop that contained personal information for 97,000 employees, the 9th Circuit found that the plaintiffs' heightened risk of identity theft fulfilled the "injury in fact" requirement. Such injury must be: a) concrete and particularized and b) actual or imminent, not conjectural or hypothetical.

More recently, the 7th Circuit twice found standing for plaintiffs in data breach class actions. See *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) and *Lewert v. PF Chang's China Bistro Inc.*, 819 F.3d 963 (7th Cir. 2016). In both instances, the affected customers received one year of credit reporting and identity theft protection. The court relied in part on the defendants' post-breach mitigation efforts as evidence of a "concrete" injury. In *Neiman Marcus*, the court noted that the provision of credit monitoring and identity-theft protection indicated a risk of future injury that was not "so ephemeral that it [could] safely be disregarded."

In *Spokeo*, which was issued after these cases were decided, the plaintiffs contended that Spokeo (a "people search engine") had violated the FCRA by publishing false information. *Spokeo* sought to defeat the action by distinguishing "procedural

violations [of statutes]...divorced from any concrete harm," which they contended do not qualify as injuries-in-fact. The Court agreed that the 9th Circuit had failed to examine whether the harm was "concrete," and remanded on that basis.

Post-*Spokeo*, plaintiffs have had some success in establishing standing in data breach class actions. In *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386 (6th Cir. Sept. 12, 2016), the 6th Circuit followed an approach similar to *Neiman Marcus*. However, unlike in *Neiman Marcus*, the plaintiffs in *Galaria* did not allege that they had already experienced fraud or identity theft, but rather claimed a past injury in relation to the costs associated with mitigating the threat of the theft of their personal information, as well as a future injury associated with the substantial risk of identity theft.

In *Galaria*, the court focused on Nationwide's offer to provide credit-monitoring and identity-theft protection as an acknowledgment of "the severity of the risk." The court determined that the substantial risk of harm was reinforced by the actions the company took to assist its customers after the breach, which justified the plaintiffs' incurred mitigation costs. For example, the court stated that "Nationwide recommended [that customers place a credit freeze on their credit reports] but did not cover [this cost for the customers]," which was a further indication that plaintiffs had sufficiently alleged "concrete injury suffered to mitigate an imminent harm."

This month, in *In Re Horizon Healthcare Services*, the 3rd Circuit found standing in a class action brought against Horizon Healthcare after a data breach compromised personal and health information. Applying *Spokeo*, the court found that the violation of a statute could inflict a concrete injury that is either tangible or intangible. The court further noted that the "unauthorized dissemination" of personal information in violation of the FCRA "constitutes a *de facto* injury that satisfies the concreteness requirement of Article III standing."

Importantly, the court disagreed with the plaintiff's contention that an offer of free credit monitoring could be taken as proof that the defendant acknowledged a significantly increased risk of injury. The 3rd Circuit noted that this would "disincentivize companies from offering credit or other monitoring services" and would be contrary to Federal Rule of Evidence 407, which excludes subsequent remedial measures as evidence of fault. Thus, while stated in dicta, the 3rd Circuit differed sharply from the 6th and 7th Circuits' treatment of the issue.

In the wake of these developments, firms must carefully assess their response plans in advance of an actual incident. Entities should also review their cyber insurance policies to determine whether they require certain post-breach mitigation measures, and be mindful of the potential consequences in follow-on litigation when crafting data breach notifications and remedial actions.

Authors

Daniel Silver

Partner

T: +1 212 878 4919

E: daniel.silver

@cliffordchance.com

Philip Lockwood

Associate

T: +1 202 912 5417

E: philip.lockwood

@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2017

Clifford Chance US LLP

www.cliffordchance.com

Abu Dhabi ■ Amsterdam ■ Bangkok ■ Barcelona ■ Beijing ■ Brussels ■ Bucharest ■ Casablanca ■ Doha ■ Dubai ■ Düsseldorf ■ Frankfurt ■ Hong Kong ■ Istanbul ■ Jakarta* ■ London ■ Luxembourg ■ Madrid ■ Milan ■ Moscow ■ Munich ■ New York ■ Paris ■ Perth ■ Prague ■ Rome ■ São Paulo ■ Seoul ■ Shanghai ■ Singapore ■ Sydney ■ Tokyo ■ Warsaw ■ Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.