Client Update
Florida Court Dismisses Data Breach Lawsuit for Lack of Standing

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Mark P. Goodman
mpgoodman@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Elliot Greenfield
egreenfield@debevoise.com

David Sarratt
dsarratt@debevoise.com

Addressing a key issue in consumer data breach class action litigation, a federal court in the Southern District of Florida has dismissed a lawsuit against a Florida hospital for lack of Article III standing because there was no allegation that the individual plaintiff's personal information had actually been misused. *See Case v. Miami Beach Healthcare Group, Ltd., et al.*, Case No. 14-24583-CIV (S.D. Fla.) (Feb. 26, 2016). This reinforces the requirement of a plaintiff's ability to plead actual harm with some specificity – a daunting task in most consumer data breach cases. Though some courts have taken a more plaintiff-friendly view of the pleading standard, *Case* pushes those decisions further toward the margins.

WHERE THE COURTS HAVE BEEN SO FAR

The starting point for most recent judicial discussion of the standing issue in data breach cases is the Supreme Court's 2013 decision in *Clapper v. Amnesty International USA*. There, the Court rejected a challenge by alleged victims of federal surveillance who could not plead that they were actually surveilled or injured: "[T]hreatened injury must be *certainly impending* to constitute injury in fact," the Court said, and "[a]llegations of *possible* future injury" are not sufficient. (emphasis in original). The Court acknowledged that, in some prior cases, it had upheld standing based on a "substantial risk" that the harm would occur. The Court went on to state in 2014, in *Susan B. Anthony List v. Driehaus*, that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."

Many lower courts have relied on *Clapper* in dismissing data breach consumer class actions at the pleading stage, holding that the alleged theft of personal information does not, by itself, establish an imminent risk of concrete injury. Even before *Clapper*, in *Reilly v. Ceridian Corp.*, the Third Circuit held that "[i]n data breach cases where no misuse is alleged, . . . there has been no injury – indeed, no change in the status quo."

Reilly involved a security breach at a payroll processing firm. A hacker gained access to the personal information of about 27,000 of the firm's customers' employees, including their names, addresses, Social Security numbers, dates of birth and bank account information. The court held that the mere accessing of that data by a hacker, and the plaintiffs' allegations of possible future injury, were not sufficient to satisfy Article III because the alleged injury was not "certainly impending."

Last year, however, the Seventh Circuit ruled in *Remijas v. Neiman Marcus Group, LLC* that "an increased risk of future fraudulent charges and greater susceptibility to identity theft" was sufficient to confer standing at the pleading stage. The data breach that Neiman Marcus experienced potentially exposed approximately 350,000 credit card numbers. Approximately 9,200 credit cards were used fraudulently, although the victims were later reimbursed for the charges. The court declined to assume that future charges would be reimbursed, and found that, in any case, there are "identifiable costs associated with the process of sorting things out."

The *Neiman Marcus* decision went against the clear trend post-*Clapper* of dismissing data breach class actions in the absence of unreimbursed economic harm that could demonstrably be connected to the particular breach in question. As we noted at the time, it remained an open question whether *Neiman Marcus* would in time be seen as a minority view or as a sign of reversal in the trend.

THE *CASE* DECISION

Case involved a data breach at a Florida hospital that allegedly exposed the names, dates of birth and/or Social Security numbers of over 85,000 of the hospitals' patients. Because the plaintiff in *Case* did not claim that her information "was actually misused, or that the unauthorized disclosure of her sensitive information caused her any type of harm, economic or otherwise," the district court last week held that she lacked standing.

The *Case* court distinguished other decisions, such as the consumer class action that followed the data breach of Target stores, on the basis that the plaintiffs in those cases alleged actual injuries, "including unlawful charges, restricted or blocked access to back accounts, inability to pay other bills, and late payment charges or new card fees."

The court also rejected the plaintiff's argument that she was injured because she did not receive the full value of the services for which she paid, which purportedly included data protection services. The court concluded that the

hospital's charges to the plaintiff for medical care did not "explicitly or implicitly include[] the cost of data protection."

SIGNIFICANCE FOR DATA BREACH LITIGATION

The *Case* decision joins a number of other post-*Neiman Marcus* decisions where consumer class actions following a data breach have failed at the motion to dismiss stage. *See*, *e.g.*, *In re SuperValu, Inc.*, No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016); *Whalen v. Michael Stores Inc.*, No. 14-CV-7006, 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015); *Fernandez v. Leidos, Inc.*, No. 2:14-CV-02247, 2015 WL 5095893 (E.D. Cal. Aug. 28, 2015). Certain cases have gone the other way at least in part, making it important to watch for additional cases as this area of the law continues to develop. *See*, *e.g.*, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 589760 (N.D. Cal. Feb. 14, 2016); *Walker v. Boston Med. Ctr. Corp.*, No. SUCV20151733BLS1, 2015 WL 9946193 (Mass. Super. Nov. 20, 2015). But it seems fair to say that the directional arrow is pointing toward treating the *Neiman Marcus* approach as the minority position.

The *Case* decision underscores the importance of scrutinizing the specific allegations relevant to the issue of future harm to individual consumers – *e.g.*, what type of data is at issue, whether it is certain that a third party accessed the consumers' data, whether the data has been made available to identity thieves, whether fraudulent charges have been made and whether those charges have been reimbursed to the consumers. By rejecting the argument that a data breach means the promised services have not been delivered at full value, *Case* also rejects a theory that – if accepted – potentially could have allowed for a much more liberal approach to standing.

* * *

Please do not hesitate to contact us with any questions.