In re: Marriott International Inc., Customer Data Security Breach Litigation

February 27, 2020

The post-data breach consumer class action against Marriott has just survived a motion to dismiss. Federal District Judge Paul Grimm's opinion adopts a newly generous (to plaintiffs) view of what sort of post-breach harm must be alleged to meet standing requirements. In contrast to the days when post-data breach cases were often dismissed at the pleading stage for lack of standing, this new decision seems likely to embolden the plaintiffs' bar to invest further in data breach litigation.

BACKGROUND

Marriott announced in late 2018 that there had been unauthorized access to the guest information database of Starwood, which Marriott acquired in September 2016. Over 300 million guests were affected. Compromised information included names, mailing addresses, phone numbers, email addresses, passport numbers, loyalty program account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, payment card expiration dates and tools needed to decrypt cardholder data.

Ten post-breach class actions were consolidated before Judge Grimm in the U.S. District Court for the District of Maryland. The consolidated cases included a variety of tort and statutory claims under the laws of Florida, Georgia, Illinois, Maryland, Michigan, New York and Oregon. On February 21, 2020, Judge Grimm ruled on Marriott's motion to dismiss. He threw out the Illinois negligence claim but otherwise sustained the complaint.

KEY TAKEAWAYS

Standing. While standing has often been an obstacle for plaintiffs bringing claims in data breach litigation, Judge Grimm accepted four separate reasons why plaintiffs' allegations of injury-in-fact were sufficient.

- **Judge Grimm held that plaintiffs adequately alleged standing on a theory of imminent risk of injury of identity theft. Even for those plaintiffs that did not plead injury-in-fact based on identity theft that had already occurred, Judge Grimm held that the combination of the plaintiffs' allegations about the targeting of personal information for the purpose of misuse in the cyberattack, along with the allegations of identity theft that had already occurred, made the threatened injury "sufficiently imminent" to establish standing.**

- **Where plaintiffs adequately pled injury-in-fact based on harm already incurred (like identity theft), Judge Grimm held that they have also successfully established injury-in-fact based on time and money spent mitigating that harm.**

- **Judge Grimm joined what he called "the growing trend across courts . . . to recognize the lost property value of [personal identifying] information." He cited statements by UK Information Commissioner Elizabeth Dunham and U.S. Attorney General William Barr as examples of persons who have identified the real value of personal data. The value of personal information is, Judge Grimm said, "not derived solely (or even realistically) by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check."**

- **Plaintiffs also successfully pled injury-in-fact by alleging that Marriott's purported misrepresentations about its data security "diminished the value of their purchases." Judge Grimm held that it is not necessary at the motion to dismiss stage to determine what portion of the bargain between hotel and customer is attributable to data security. Rather, plaintiffs could plead injury-in-fact simply by alleging that "there was an explicit or implicit contract for data security, that plaintiffs placed value on that data security, and that Defendants failed to meet their representations about data security."**

Negligence. The only claim Judge Grimm dismissed was a negligence claim under Illinois law. Judge Grimm held that no common-law duty regarding data security has been recognized under Illinois law.

Breach of Contract. Plaintiffs did not need to allege that "they read, saw, or understood the Privacy Statements" in order to state a claim for breach of contract. It was enough that plaintiffs alleged that "they assented to [the] offers by staying at Marriott and Starwood properties, enrolling in the SPG Program, and providing their personal information to Marriott and Starwood."

9(b) Heightened Pleading. For the statutory claims that sounded in fraud (which include the Maryland Consumer Protection Acts claims, the California Unfair Competition Law claims and the New York General Business Law claims), plaintiffs were required to meet the heightened pleading requirement of Federal Rules of Civil Procedure 9(b). Judge Grimm held that plaintiffs met this requirement by alleging that "Marriott knew or should have known about its allegedly inadequate data security practices and the risk of a data breach" and that plaintiffs would not have paid Marriott or would have paid it less had they known the truth about the alleged omissions.

WHAT'S NEXT?

On the same day Judge Grimm issued his opinion, he also issued an order asking counsel to confirm their availability for a settlement conference to be held on March 31, 2020. Counsel for other related cases, including the securities and derivative suits that had been stayed pending decisions on motions to dismiss in other related cases, were asked to join the settlement conference as well.

Judge Grimm's detailed opinion demonstrates a willingness to allow litigation arising out of data breaches to proceed to discovery. Judge Grimm specifically distinguished earlier Fourth Circuit decisions where post-breach claims failed at the pleading stage; here, in contrast, Judge Grimm held that plaintiffs' complaint contained sufficient allegations regarding the targeting of personal information for misuse.

Judge Grimm also rejected a number of arguments raised by Marriott as being premature at the motion-to-dismiss stage. For example, Judge Grimm held that it was too early in the case to determine what portion of the alleged bargain between plaintiffs and Marriott could be attributed to data security. Additionally, Judge Grimm held that, while Marriott may be able to argue after discovery that the injuries plaintiffs alleged were not caused by the data breach, he would not dismiss the plaintiffs' claims on grounds of traceability.

An uptick in data breach litigation in California has been expected, with the California Consumer Privacy Act and its private right of action for data breaches now in effect. Judge Grimm's approach, if accepted by other courts, could portend a relaxation of standing requirements that would encourage class action litigation in a range of forums.

*** * ***

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Lisa Zornberg
lzornberg@debevoise.com

Suchita Mandavilli Brundage
smbrunda@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com