BRACEWELL

INSIGHTS

Data Breach Lawsuit Survives Motion to Dismiss

April 28, 2017

In an April 13, 2017 decision in *Walters v. Kimpton Hotel*,[1] a California federal judge rejected the bid of hotel chain Kimpton Hotel and Restaurant Group, LLC to dismiss a proposed class action arising from a data breach last year. Judge Vince Chhabria found that the named plaintiff sufficiently alleged imminent harm to establish standing notwithstanding the absence of allegations that his personal information had been misused.

Background of the Lawsuit

In August 2016, Kimpton Hotel disclosed that malware had been installed on its servers from February 16, 2016 to July 7, 2016, and mailed notification letters to those guests who used their payment cards at a front desk during that period. Plaintiff Lee Walters was a guest at a Kimpton Hotel on May 29, 2016. Walters alleged that, following his stay at the hotel, his payment card information was stolen. Walters further alleged that, after learning of the breach, he expended time and effort to monitor his credit, and that he faced increased risk of identity theft due to the server breach.

The Decision

Judge Chhabria found that a plaintiff does not need to "actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes," and that Walters' allegations of imminent harm were sufficient to confer standing to survive Kimpton's motion to dismiss. Judge Chhabria adopted the standing approach applied by the Sixth and Seventh Circuits in *Galaria v. Nationwide Mut. Ins. Co.* and *Lewert v. P.F. Chang's China Bistro*.[2]

In *Galaria*, the Sixth Circuit held that allegations of a continuing, increased risk of fraud and identify theft were more than just speculative allegations of injury, emphasizing that there is "no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."[3] Similarly, in *P.F. Chang's*, the Seventh Circuit explained that "it is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is sooner or later to make fraudulent charges or assume those consumers' identities."[4]

Additionally, Walters' allegations of purchasing credit-monitoring services and other out-of-pocket expenses were actual damages sufficient to allow claims of breach of implied contract, negligence, and a violation of California's unfair competition law to survive. The breach of implied contract claim was based on allegations that Kimpton's privacy policy, which states that the company is committed to protecting customer personal data, created an enforceable promise to customers in that it was a voluntary duty and constituted valid consideration.

Takeaways

It is important to note that a court at the motion to dismiss stage must accept allegations of

imminent harm as true, and it is far from clear whether Walters will be able to prove injury-in-fact going forward. Even so, this decision is yet another reminder that companies can no longer assume that consumer-initiated lawsuits will be dismissed where no customer information has yet been misused, and they must prepare for legal attacks from all sides – regulators, shareholders, and consumers – even as they work to resolve the fallout from a cyberattack. A great starting point for all companies is a simple and straightforward incident response plan that anticipates the inevitable cyber breach. Such a plan can provide a framework for integrating a response amongst the company's management, IT, legal, external communications, and outside experts, such as legal counsel and cyber forensic investigators.

A copy of the decision is available ***here***.

---

[1] *Walters v. Kimpton Hotel & Rest. Grp., LLC*, No. 16-CV-05387-VC, 2017 WL 1398660 (N.D. Cal. Apr. 13, 2017).

[2] *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016). While not cited by the judge, the Ninth Circuit also recognizes that, following the theft of unencrypted personal data, an increased risk of identity theft constitutes harm. *See Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

[3] *Galaria*, at 388.

[4] *P.F. Chang's*, at 967 (internal citations omitted).