GODFREY & KAHN S.C.

Data Privacy & Cybersecurity Flash

Douglas M. Poland
608.284.2625
dpoland@gklaw.com

Melissa M. York
414.287.9336
myork@gklaw.com

Standing requirement of actual or imminent injury continues to thwart data breach lawsuits

In the past year, breaches of systems containing personal information and data have seen a startling increase and achieved ever-greater public attention and notoriety. Starting with the Target data breach revealed in December 2013 and continuing through the revelation in September 2014 that account information for more than 50 million credit card holders had been pilfered through a breach of Home Depot's point-of-sale data payment systems, the frequency of such incidents indicates that personal financial and other information is widely susceptible to theft from the merchants and other entities that use and store that data. Following on the heels of these well-publicized breaches, individuals and businesses whose information and data have been exposed to breaches by unauthorized users, or actually exfiltrated by those who have accessed it, have filed lawsuits against the entities whose systems were breached. These lawsuits have presented courts with questions of first impression related to data security law. A threshold issue raised by many of these lawsuits is whether the owners of information or data that is accessed or misappropriated have legal standing to bring private tort claims when the only alleged harm is the potential that their payment card data and personally identifiable information have been disclosed as part of a data breach.

Under both state common law and federal constitutional law, to have standing to maintain a court action a plaintiff must show injury in fact that is either actual or imminent. In 2013, the Supreme Court clarified in *Clapper v. Amnesty International, USA*[1] that to qualify as "imminent," the "threatened injury must be certainly impending." Most plaintiffs in data breach cases assert that injury is "imminent" because they have been exposed to an increased risk of future fraudulent credit card charges and an increased risk of identity theft. In addition, many plaintiffs assert "actual" injuries, including the loss of time and money associated with resolving fraudulent charges, the loss of time and money associated with protecting against the risk of future identity theft, the financial loss they suffered from having purchased products that they wouldn't have purchased had they known of the defendants' misconduct, and the loss of control over and value of their private information.

With few exceptions,[2] courts have consistently failed to see merit in arguments that plaintiffs have injury, whether imminent or actual, when their data was potentially accessed by an unauthorized user but there is no proof it has yet been fraudulently used. Representative of

The information in this article is based on a summary of legal principles. It is not to be construed as legal advice. Individuals should consult with legal counsel before taking any action based on these principles to ensure their applicability in a given situation.

[1] 133 S. Ct. 1138 (2013).

[2] *See, e.g., Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (declining to extend the *Clapper* imminence standard); *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, MDL No. 11-md-2258, 2014 WL 223677, at *8-9 (S.D. Cal. Jan. 21, 2014) (rejecting argument that *Clapper* overruled Ninth Circuit President); *see also Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (identifying circuit split pre-*Clapper* over whether increased risk of harm stemming from a data security breach constitutes an Article III injury).

such rulings is the opinion issued recently in *Remijas v. The Neiman Marcus Group, LLC*,[3] in which a federal judge in Illinois dismissed a class action related to a data breach on the grounds that the plaintiffs had failed to state a claim. In *Remijas*, the Nieman Marcus Group's servers were breached by hackers, resulting in the potential disclosure of 350,000 customers' payment card data and personally identifiable information. The plaintiffs alleged that Nieman Marcus failed to adequately protect against a security breach. Relying on *Clapper,* the court dismissed the case for lack of standing, holding that there was not a plausible inference that any of the 350,000 customers were at a "certainly impending" risk of identity theft. Although the court acknowledged there was an imminent risk of fraudulent charges (because customer information had already been fraudulently used for 9,200 of the customers), it held that even as to the 9,200 card holders whose cards had been used for unauthorized credit card charges, such charges are not sufficiently "concrete" injuries to confer standing because the plaintiffs failed to allege that they would be held financially responsible for those charges. In addition, the court noted that standing does not exist where plaintiffs allege they spent money towards mitigating risk of future fraudulent charges, reasoning that the underlying harm the plaintiffs were seeking to avoid is not a cognizable Article III injury.

Although data breaches such as those experienced by Target, Nieman Marcus, and Home Depot are embarrassing and tremendously costly for the retailers, inconvenient for their customers, and can lead to regulatory actions by state and federal authorities, the holders of data that is exposed in a breach remain largely immune from lawsuits by the owners of that data because of the "actual or imminent" injury standing requirement. Nonetheless, the continued proliferation of data breaches will undoubtedly lead to more lawsuits by the owners of data that is exposed in such breaches, as well as to further development in the law governing standing in such lawsuits.

---

[3] *Remijas v. The Neiman Marcus Group, LLC*, Case No. 14 C 1735, the Illinois Northern District United States District Court for the Northern District of Illinois, Eastern Division (September 19, 2014).

Data Privacy & Cybersecurity Practice Group

Team Leaders

Richard Marcus
rmarcus@gklaw.com

Douglas Poland
dpoland@gklaw.com

Team Members

Sean Bosack
sbosack@gklaw.com

Brian Cahill
bcahill@gklaw.com

Christopher Cahlamer
ccahlamer@gklaw.com

James Friedman
jfriedman@gklaw.com

Kerry Gabrielson
kgabrielson@gklaw.com

David Gilles
dgilles@gklaw.com

Kristen Irgens
kirgens@gklaw.com

Nicholas Kees
nkees@gklaw.com

Andrew Landsman
alandsman@gklaw.com

Scott LeBlanc
sleblanc@gklaw.com

John McDonald
jmcdonald@gklaw.com

Patrick Murphy
pmurphy@gklaw.com

Todd Smith
tsmith@gklaw.com

Scott Thill
sthill@gklaw.com

Peter Wilder
pwilder@gklaw.com

Eric Wilson
ewilson@gklaw.com

Melissa York
myork@gklaw.com