Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Clapper Defense No Sure Bet In Home Depot Breach Suits

By **Allison Grande**

Law360, New York (September 11, 2014, 8:45 PM ET) -- Home Depot Inc. is likely to point to the U.S. Supreme Court's landmark Clapper ruling to fend off the class actions piling up over its recent data breach, but attorneys say plaintiffs are quickly learning that they can bypass the defendant-friendly 2013 decision by proving that their data has been misused or that they relied on false security pledges.

Consumers in Georgia filed the first class action against Home Depot on Sept. 4, four days before the home improvement retailer confirmed that hackers had breached its customers' payment card data. Since the confirmation, consumers in Illinois and Missouri have brought three more class actions over the breach.

The wave of litigation is consistent with the response the plaintiffs bar has had to similar high-profile breaches at companies such as Target Corp., Sony Corp., Barnes & Noble Inc., P.F. Chang's China Bistro Inc. and Michaels Stores Inc., which also saw the first suit filed against it before it had verified a data breach.

“The fact remains that if you get breached, you can count on getting sued,” Steptoe & Johnson LLP partner Jason Weinstein told Law360.

To fend off breach litigation, companies have turned to the Supreme Court's pivotal 2013 decision in Clapper v. Amnesty International, which established that to satisfy Article III standing requirements, plaintiffs need to prove they have suffered actual harm or a “certainly impending” injury.

While the Clapper case centered on the plaintiffs' ability to challenge a sweeping government surveillance law, the ruling has proved to have a much broader application. It has been useful to companies defending against data breach claims, which typically involve scenarios where consumer data has been improperly accessed but not necessarily misused.

“Clapper hasn't eliminated privacy class actions, but generally speaking, Article III standing post-Clapper has been a strong and significant defense in instances where plaintiffs can't allege imminent or credible actual injuries,” Mayer Brown LLP attorney Evan Wooten said. “It's oftentimes probably the best line of defense for most companies that have been victimized by a data breach.”

While Home Depot has yet to respond to the data breach claims pending against it, attorneys anticipate that the retailer is likely to follow in the footsteps of its predecessors by citing the Clapper argument.

“Home Depot looks to be the same as other recent high-profile retailer data breaches, so it may play out like those suits,” said Judy Selby, the co-chair of BakerHostetler's information governance team. “It's been pretty clear that the effect of Clapper has been to provide greater ammunition to the defense.”

But attorneys are quick to note that, while the decisions to date have for the most part favored defendants, companies would be wise not to get a false sense of security from the first wave of post-Clapper cases.

“One important takeaway from the past year of data breach litigation is that plaintiffs’ lawyers adapt — and that’s what they’re doing here,” Weinstein said. “We see class action lawyers looking for creative ways to plead injury and adding other causes of action — under state or federal law — that might avoid the need to demonstrate actual or imminent injury.”

Before Clapper, the uncertainty surrounding Article III standing led courts to issue mixed decisions on whether the threat of compromised data being misused by thieves was enough to allow plaintiffs to proceed with their claims.

But the Supreme Court's ruling has whittled away at much of the divide, attorneys say.

“Clapper changed the landscape by really tightening up and clarifying what the standard is for standing,” said Montgomery McCracken Walker & Rhoads LLP partner John Papianou.

During the past year, courts across the country have issued several decisions that have applied Clapper to support the dismissal of data breach class actions on standing grounds.

In September 2013, an Illinois federal judge tossed a putative class action against Barnes & Noble over a security breach affecting PIN pad devices in 63 of its stores after concluding that none of the plaintiffs had shown they were actually harmed by the incident.

A Kansas judge in February also dismissed two proposed class actions filed in the wake of a data breach at Nationwide Mutual Insurance Co. on the grounds that there was no evidence anyone had been harmed. And a D.C. federal judge in May gutted a wide-ranging multidistrict case over a breach involving security contractorScience Applications International Corp. after finding scant evidence of harm from the loss of patient medical files.

“Clapper has certainly made it harder for the plaintiffs' bar to come up with allegations to overcome the requirement that the injury needs to be more than speculative,” Selby said.

However, attorneys on both sides of the bar noted that plaintiffs were starting to develop creative arguments and choose plaintiffs more carefully to get around that hurdle.

“Although some courts have used [the Clapper decision] to dismiss data breach cases brought under older theories such as risk of future harm, those theories generally don't survive regardless,” plaintiffs' attorney Jay Edelson of Edelson PC said. “The modern trend is to establish that the failure to take necessary precautions diminished the value of the good or service provided. Clapper has nothing to say on that theory whatsoever.”

Plaintiffs attorneys have also found success in preserving at least some claims at the dismissal stage by shifting their focus to plaintiffs who have paid for services or suffered demonstrable identity theft that

has resulted in unreimbursed losses, attorneys noted.

“Both of those scenarios make the standing argument more difficult for defendants to win,” said Al Saikali, the co-chair of the data security and data privacy practice atShook Hardy & Bacon LLP.

One of the most significant rulings for the plaintiffs' bar came in January, when a Southern District of California judge preserved the plaintiffs' standing and security claims in a proposed class action over a massive breach involving Sony Corp.'s PlayStation network. The parties have since agreed to settle for $15 million.

While the judge nixed 43 of 51 claims in the plaintiffs' first amended class action complaint, he did rule that the plaintiffs' allegations that their personal information was collected by Sony and then wrongfully disclosed as a result of the 2011 intrusion was sufficient to establish standing.

A March ruling by a Northern District of California judge that allowed a putative class action over LinkedIn Corp.'s 2012 data breach to proceed also lent weight to plaintiffs' prospects of using the argument that a company made security misrepresentations in its privacy policy to overcome standing hurdles, attorneys noted. That case has also since been settled, for $1.25 million.

Moving forward, attorneys anticipate that the plaintiffs bar will continue to refine its strategies for dodging Clapper, which also include citing privacy statutes that provide for damages without having to prove actual harm.

And plaintiffs are likely to receive help from the Supreme Court's June decision in Susan B. Anthony List et al. v. Steven Driehaus as well as the increasing prominence and visibility of hackers. Papianou noted the plaintiffs bar had already begun to cite the Susan B. Anthony List case to show that an injury only has to be substantially likely.

“As the types of data breaches and hackers become more sophisticated, we are likely to see more diverse and sophisticated theories,” Wooten said. “In certain cases, hackers have taken responsibility for a breach and made public statements about what they might do with the data, which plaintiffs could use to help fill in the causal chain and could certainly change the calculus for the courts.”

--Editing by Kat Laskowski and Emily Kokoll.
