Bloomberg BNA

Privacy Law Watch™

VOL. 16, NO. 234 DECEMBER 6, 2016

Litigation

How Much Harm From a Breach Is Enough? Question May Head to High Court in 2017

■ *Companies facing data breaches grapple with lack of clear harm standard for consumer class actions*

■ *Breach harm standing has potential to reach U.S. Supreme Court in 2017*

Hacking attacks, lax data security and rampant cybercrime create risks for corporations, including consumer lawsuits stemming from large-scale data breaches.

Plaintiffs have lined up at courthouse doors for years, seeking damages from companies like Target Corp., The Home Depot Inc., Sony Pictures Entertainment Inc. and The Wendy's Co.

But those claims have yet to bring a wave of winning class actions on the merits. Many are either tossed out of court in the preliminary stages or are settled before the full facts of the breach are discovered.

2017 may be the year the U.S. Supreme Court is asked to review a stumbling block for data breach class claims: the need to show that the breach of a person's data caused him or her to suffer legally recognizable harm. Without a harm showing, plaintiffs lack the legal standing to proceed with their claims.

Businesses want clarity on the harm standard because of the frustratingly high number of data breach cases filed, Stephen Lilley, a corporate defense-side cybersecurity and data privacy attorney at Mayer Brown LLP in Washington, told Bloomberg BNA.

There is a concern among companies that there are ''too many lawsuits filed without any real harm to consumers,'' he said.

Stakes High. The stakes are high. In addition to consumer class claims, companies that have been hit with data breach claims also face the possibility of lost customer confidence, bad press, jeopardized trade secrets, state attorney general actions, attorney fees, pricey breach notifications, years of free credit monitoring and other breach clean-up costs.

Clarification from the Supreme Court of the data breach harm standard would be a boon to companies that need to evaluate the risks associated with data breaches, and could profoundly influence how much companies spend to prevent breaches. It may also be a deciding factor for law firms weighing whether to settle or gear up for expensive litigation.

Varying circuit court rulings on the harm plaintiffs need to show in data breach cases have many privacy professionals hoping for a clearer rule in 2017.

It is ''very likely'' that the Supreme Court will ''in the near future'' hear a data breach standing case to clarify the unsettled standard, James Westerlind, cybersecurity counsel at Arent Fox LLP in New York, told Bloomberg BNA.

In fact, a recent putative data breach class claim from the U.S. Court of Appeals for the Sixth Circuit case involving Nationwide Mutual Insurance Co. is a candidate for high court review next year, he said.

Mega Hacks, Recourse Unclear. Companies that collect, handle, store and dispose of massive amounts of consumer data face a high risk for breach class actions.

Yahoo! Inc., for example, was hit with multiple class actions stemming from a September data breach that impacted over 500 million accounts. Multiple federal court actions were filed, resulting in a pending multidistrict case.

The Supreme Court clarified the general harm standard in *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013) and *Robins v. Spokeo, Inc.*, 136 S. Ct. 1540 (2015) to mean that harm must be concrete and particularized and that an alleged future risk of harm must be substantial or certainly impending. Neither of the cases involved a data breach.

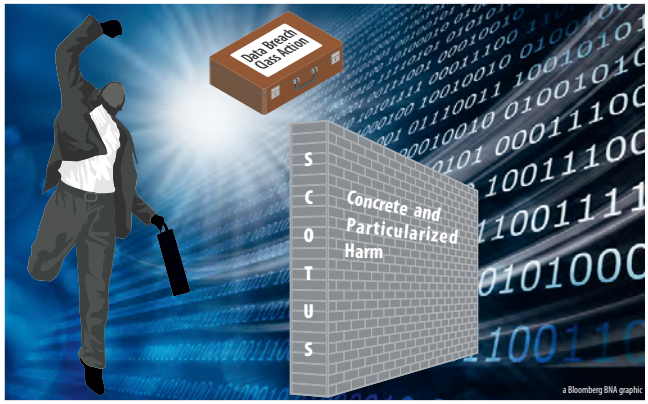
Tanya Forsheit, partner and co-chairwoman of the Privacy & Data Security group at Frankfurt Kurnit Klein & Selz in Los Angeles, told Bloomberg BNA that courts have reached varying conclusions on data breach harm since *Clapper* and *Spokeo* because those cases didn't involve a data breach and were based on statutory damages.

It would be helpful for companies and consumers facing data breaches to have a standard that came from a case that alleged harms or involved a statute that didn't provide for statutory damages, she said.

Even if a plaintiff is able to successfully plead harm in a data breach suit, there's no guarantee that a judge won't toss the suit at a later stage of trial. In most cases, plaintiffs still need to plead adequate harm, because many laws and causes of action require actual injury as part of the claim.

Defendant companies are left with uncertain litigation risk assessments, leading many to settle consumer

 ISSN 0000-0000



class actions, but not before incurring substantial litigation costs.

Circuit Court Inconsistencies. Federal district courts have relied on varying approaches to data breach standing from the federal circuit courts, such as the Third, Sixth, Seventh and Ninth Circuits, which has led to a patchwork of consumer data breach harm opinions.

Forsheit said that courts have ruled inconsistently in data breach harm cases ''with respect to whether increased risk of future harm is sufficient by itself to support'' federal standing.

Because of the ''lack of clarity since *Clapper*,'' the data breach harm ''standard could absolutely benefit from further clarification as to when increased risk of future identify theft provides a basis for standing,'' Forsheit said.

The Seventh Circuit has ruled that a likely threat of identity theft is enough harm to give plaintiffs legal standing if the alleged harm is somehow traceable to the data breach.

These cases tend to fail if harm from the data breach is too disconnected from the breach.

Absent a clear data breach harm standard, too many lawsuits are filed without any real harm to consumers.

STEPHEN LILLEY, CYBERSECURITY AND DATA PRIVACY ATTORNEY
MAYER BROWN LLP, WASHINGTON

Meanwhile, the Sixth Circuit ruled in *Galaria v. Nationwide Mutual Insurance Co.* that a substantial risk of harm, along with reasonable incurred mitigation costs, were concrete enough to establish harm.

A three-judge Sixth Circuit panel ruled against a putative class that sued Nationwide over claims that the insurance company didn't adequately protect its personal information in an October 2012 data breach that affected 1.1 million consumers' sensitive data.

On Oct. 12, the appeals court declined to have the case reheard by the full Sixth Circuit bench. The putative class will have 90 days from the entry of the Oct. 12 judgment to appeal to the Supreme Court.

Westerlind said that the *Nationwide* decision missed the mark because it ''violates the well-settled standing rule that where alleged future injury is contingent on the decisions and actions of unknown third-parties, there is no injury-in-fact.''

Test Case Ahead in '17? Westerlind said that the Sixth Circuit's *Nationwide* case may be poised for high court review, but he didn't expect the justices to uphold the circuit court's decision.

The ''Supreme Court doesn't seem inclined to expand the scope of standing'' and may hear a data breach standing case ''to clarify the law in this regard and put an end to the growing split among circuit courts,'' he said.

Lilley, who represented Spokeo, said that absent a test case in 2017, both plaintiff and defense attorneys presented with a data breach standing case ''should be thinking about how to frame these issues in the district court'' to better prepare themselves for an eventual appeal for the circuit courts and the Supreme Court.

Forsheit agreed that a Supreme Court test case needs to be more pointed toward data breach cases and should ''avoid some of the complexities of Spokeo.'' Any case to clarify this issue should directly focus on ''the harm standard for standing in data breach cases,'' she said.

For both companies and consumers, there needs to be a ''baseline'' rule, Forsheit said.

BY DANIEL R. STOLLER

To contact the reporter on this story: Daniel R. Stoller in Washington at dstoller@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

  PRA ISSN 0000-0000