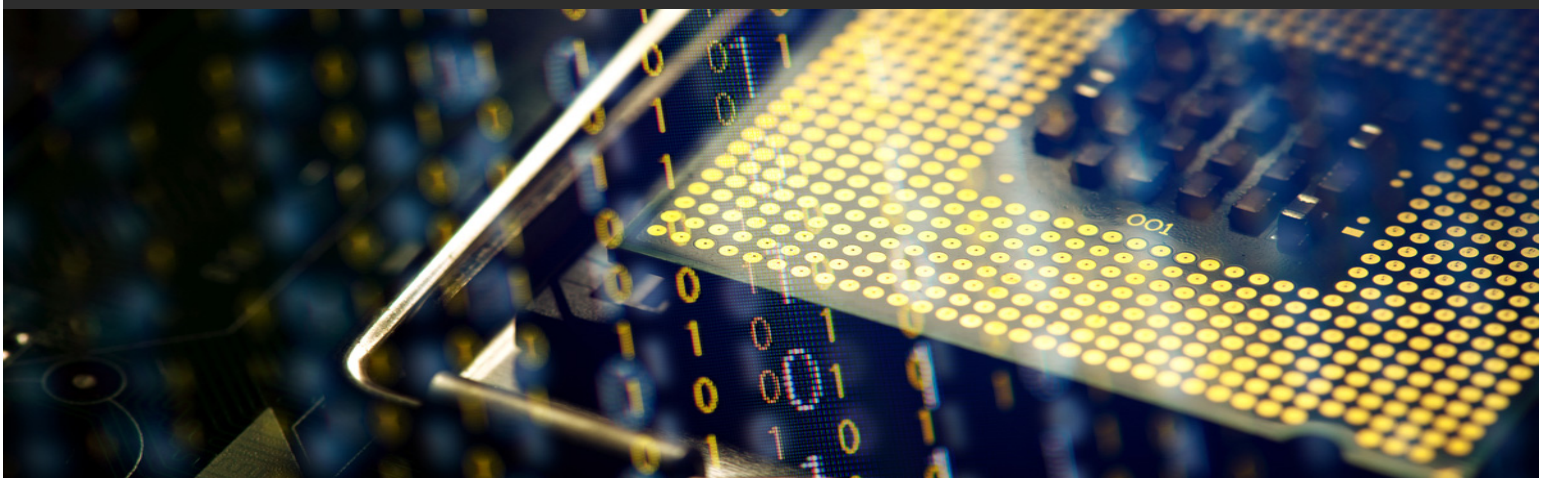
GT GreenbergTraurig

The 50-State Cybersecurity Class Action Is Here to Stay. How to Defend Against It!



In recent years, plaintiff class actions lawyers have shifted their focus in cybersecurity cases from pleading federal claims to asserting claims under state law of residents of all 50 states. However, this potentially raises class certification issues that make these claims difficult for plaintiff to succeed on. How should one prosecute them? How should one defend them? How could one plead and prove that the plaintiffs were injured because of the breach?

By Paul Ferrillo| **March 1, 2019** | **New York Law Journal**

In recent years, plaintiff class actions lawyers have shifted their focus in cybersecurity cases from pleading federal claims to asserting claims under state law of residents of all 50 states. However, this potentially raises class certification issues that make these claims difficult for plaintiff to succeed on. How should one prosecute them? How should one defend them? How could one plead and prove that the plaintiffs were injured because of the breach? All these questions were debated strongly, litigated in various courts on a one-off basis, and were the result of several court opinions on their potential merits. The recoveries were slim. The plaintiffs' chances for success? Mediocre at best even for the big ones.

Things have significantly changed over the years, especially for defendants. For instance, Statutory Article III standing, once a big issue, is now less of an issue in some courts. Cybersecurity class actions have now graduated elementary school, beginning November 2017 with one of the first national cybersecurity class actions brought by residents of all 50 states. "The complaint is an ambitious 322-page document that names plaintiffs from every state and the District of Columbia who claim to have been

© 2019 Greenberg Traurig, LLP

injured to varying degrees by the Equifax security breach." See Tara Swaminatha, "Equifax now hit with a rare 50-state class-action lawsuit," CSO Online (Nov. 22, 2017).

Today, there are others. Are nationwide federal court, cybersecurity class actions here to stay? One may posit they are, until the U.S. Supreme Court or a Circuit Court says they are not viable or makes them too difficult for a plaintiff's counsel to proceed in an economically rational fashion.

But that raises the second question: How can you defend against them? Though this area of the law is very new, here are some suggestions on how to potentially defeat this sort of nationwide class action—especially when it comes to the issue of predominance.

Standing

The "case or controversy" requirement of Article III, §2 generally requires that a plaintiff establish "standing," i.e., an "injury-in-fact that is concrete and particularized" and "actual or imminent" and not mere conjecture.

In early cases, the "actual or imminent" harm requirement spelled doom to plaintiffs in data breach class actions. Though data may have been lost or stolen, plaintiffs sometimes could not show or plead it was misused and that they resultantly suffered a "loss." Historically, however, courts have tended to either have broad views or narrow views of what constituted true loss. In Spokeo v. Robins, the U.S. Supreme Court reversed and remanded a decision of the Ninth Circuit, holding that the Article III injury that must be plead must be both "concrete and particularized." However, the holding was more complicated than that. The Supreme Court noted that though "concrete" suggested real harm, concrete did not mean the harm needed to be "tangible" as well. Indeed, intangible harm if not risk of harm can satisfy as concrete harm under Article III. The court concluded, however, that mere violation of a statutory or procedural right alone was not enough. The violation of the right must also cause the plaintiff to suffer some sort of real world harm. Another Supreme Court case, Clapper v. Amnesty Int'l USA, 133 S.Ct 1138 (2013) did nothing to lower the standing bar for plaintiffs. In Clapper, the question was whether the allegation by a plaintiff of future injury could confer standing. The Supreme Court held that the plaintiff would have to demonstrate that injury is "certainly impending."

Courts have diverged in their application of the "concrete" harm pleading requirement. Some courts (e.g., Second, Fourth and Eighth Circuits) have held that there is no Article III standing where there is no actual identity theft or fraud that occurs as a result of the breach. In one case, Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017), the Fourth Circuit held that under existing precedent, the "risk of" identity theft is too speculative to confer standing. See also In re SuperValu, 870 F.3d 763 (8th Cir. 2017) (mere future risk of injury was not enough to confer standing); Whalen v. Michaels Stores, (2d. Cir. 2017) (plaintiff had not suffered a "particularized and concrete injury" because any resulting fraudulent charges had been reimbursed).

The Third, Sixth, Seventh, Eleventh and D.C. Circuits diverge away from decisions such as Beck v. SuperValu and take a less onerous view of what constitutes "injury." For instance, in Galaria v. Nationwide Mutual Insurance Company, No. 15-3386, (6th Cir. 2016), where there was a theft of insurance information of more than one million customers, the court found that, even though it was not "literally certain" that the data breach would cause harm to customers, there was a sufficiently substantial risk of injury, noting that when hackers specially target personal information, it is a "reasonable inference" that the data will be used for fraudulent purposes. See also Attias v. Carefirst, 865 F.3d 620 (D.C. Cir. 2017) (reversing the district court's dismissal for lack of standing, finding that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege

© 2019 Greenberg Traurig, LLP

was taken"); see generally Ian C. Ballon, Defending Security Breach Class Action Litigation, Ch. 27, E-Commerce and Internet Law: A Legal Treatise With Forms, Second Edition (Thomson/West Publishing 2018) (noting differences among the circuits on standing in cybersecurity class actions).

Conflicts of Laws and Rule 23(b)(3)'s Predominance Requirement

If a plaintiff can get over the Article III standing issue by pleading harm by showing injury or a substantial risk of injury, then what other issues are present which could derail his or her case? Well, it would be the basics of Rule 23. The most common prong of contention is Rule 23(b)(3), which states:

(b) Types of Class Actions. A class action may be maintained … if:

(3) the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.

The words "common" and "predominate" spell out the problem with 50-state cybersecurity class actions: Who is involved? How were they injured (if at all)? And what law applies to their claims? Justice Antonin Scalia's majority U.S. Supreme Court opinion in Comcast v. Behrend, 569 U.S. 27 (2013) reaffirmed the basics of the court's Rule 23 analysis: that "[t]he class action is 'an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only' … To come within the exception, a party seeking to maintain a class action 'must affirmatively demonstrate his compliance' with Rule 23." To determine whether this requirement is met, it "may be necessary for the court to probe behind the pleadings" by engaging in "a rigorous analysis" that may "overlap with the merits of the plaintiff's underlying claim." The court applied these principles to the analysis of Rule 23(b), concluding that "[i]f anything, Rule 23(b)(3)'s predominance criterion is even more demanding than Rule 23(a)."

State laws could vary when you consider that at some point all 50 states' data breach laws might be at issue. That was the point of two recent decisions. Thought it is not a cybersecurity breach case, In re Hyundai and Kia Fuel Economy Litigation is instructive. The case involved a discussion of the predominance aspects of Rule 23(b)(3) in the context of the settlement of a nationwide class action dealing with allegations of fuel economy of certain models of the defendants' cars. Though the District Court certified a proposed settlement of the class, certain plaintiffs (most notably the Virginia plaintiffs) objected to the settlement on the grounds that the District Court did not analyze differences in the 20 state consumer protection laws at issue. The Ninth Circuit reversed and vacated, noting that the failure to ascertain differences in state law was in error (in the settlement context), as differences in state law could "swamp" any common issues and defeat Rule 23's predominance requirement.

This holding makes sense. What if, for example, the laws of one state (State 1) provide for a damages standard and standard of liability far less onerous that the laws of other states (e.g., States 2, 3 and 4)? But the numbers of citizens in States 2, 3 and 4 dwarf State 1, and the laws of States 2, 3 and 4 put far more hurdles upon a plaintiff seeking to recover. How would a federal court deal with such varying individual state laws? Should all these claims be litigated together as a class? That was the point of Hyundai and Kia, and that is the point of Rule 23. This case is now back to the Ninth Circuit on an en banc appeal. The facts in Langan v. Johnson & Johnson, No. 17-1605 (2d Cir. 2018), a consumer class action, were a little different (the case was not in settlement mode), but the results were the same. The court held that plaintiffs in a class action have the burden to demonstrate that variations in state laws "do not predominate over the similarities." In a 50-state cybersecurity class action, there could indeed be variations in many states' cyber laws, creating the same underlying problem in Hyundai and Langan.

© 2019 Greenberg Traurig, LLP

Conclusion

Though standing remains an obstacle to the nationwide cybersecurity class action, its effect has been both good and bad to plaintiffs and defendants. The "predominance" of the cybersecurity laws that apply to the class action now appears to be the new game in town. We will see who wins.

Reprinted with permission from the March 1, 2019 edition of the New York Law Journal © 2019 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 1.877.257.3382 or reprints@alm.com.

About the Author:

Paul Ferrillo is a shareholder in Greenberg Traurig's cybersecurity, privacy and crisis management practice in New York City. He focuses his practice on cybersecurity corporate governance issues, complex securities and business litigation, and internal investigations.

Paul Ferrillo
ferrillop@gtlaw.com