Cybersecurity Law Report
An Acuris company

cslawreport.com

February 6, 2019

STANDING

The New Normal: Easier Data Breach Standing Is Here to Stay

By Jon R. Knight, *Boies Schiller Flexner*

The year 2018 produced what can only be described as a global explosion in data breaches. According to Business Insider, the top ten data breaches in 2018 impacted almost 2.5 billion users globally. In other words, almost one-third of the global population were victims of a data breach in 2018, absent overlap between the users impacted by the breaches. Those top breaches cut across business models and economic sectors, hitting airlines, hotels, social media, health, fitness, phone and other industries.

The year 2018 also saw the continuation of a legal trend we previously wrote about in the Cybersecurity Law Report: courts post-*Spokeo* Inc. v. Robins are more willing to find that data breach plaintiffs have demonstrated Article III standing even though they have not suffered actual monetary damages or been the victim of identity theft. While some district courts still push back on the more creative standing arguments, the bottom line is that more than half of the federal appellate courts have now addressed questions of data breach standing post-*Spokeo*, and all circuits that considered the issue in 2018 found standing existed.

These data points – the increase in the size and scope of data breaches and the increase in the likelihood that plaintiffs will be able to show Article III standing – provide helpful reminders to in-house counsel, InfoSec teams and C-suite personnel of several axioms for our digital, global economy: data breaches happen and data breach litigation will not be easy to terminate.

There is, however, a wild card. The Supreme Court recently took a question regarding *cy pres* class-action settlements (in *cy pres* settlements, damages are awarded to charitable causes instead of the plaintiffs) and transformed it into examining whether the plaintiffs had suffered a concrete injury sufficient for Article III standing. While it remains to be seen if the Court will issue an opinion that addresses the standing question, any such opinion could either accelerate or stymie the current trend toward a lower bar for Article III standing in data breach cases.

In the year-and-a-half that followed the Supreme Court's decision in *Spokeo*, six federal appellate circuits considered the issue of standing for data breach plaintiffs. The Third, Sixth, Eighth, and D.C. Circuits all found

standing, even though plaintiffs alleged little-to-no pecuniary harm and any future harm was not clearly tied to the defendant's breach or conduct. The result is an effectively lower bar for Article III standing for these plaintiffs.

The Second and Fourth Circuits, on the other hand, were more skeptical of lowering the bar, did not find standing and expressed the need for clear allegations of misuse of personal information by the purported thief.

See also "Third and Seventh Circuits Shed New Light on Spokeo Standing Analysis" (Feb. 8, 2017); "Eighth Circuit Sides With Defendants As the Spokeo Standing Battle Continues" (Oct. 5, 2016); "Spokeo's Impact on Data Breach Cases: The Class Action Floodgates Have Not Been Opened, But the Door Has Not Been Locked" (May 25, 2016).

Circuit Courts Finding Standing in 2018

In 2018, the voices of both the Seventh and Ninth Circuits were added to this debate when they found standing for data breach plaintiffs. Both of these courts uniformly supported a more open approach to standing for data breach plaintiffs.

Dieffenbach v. Barnes & Noble, Inc.

It was not entirely unsurprising that the Seventh Circuit found data breach plaintiffs to have Article III standing. After all, the circuit had already found in the pre-Spokeo universe that the theft of personal information presumed an increased risk of future injury. In *Remijas v. Neiman Marcus Grp., LLC*, the circuit rhetorically asked "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." But *Dieffenbach v. Barnes & Noble, Inc.* provides additional examples of non-traditional harms that courts will consider as injury for both standing and damages purposes.

In *Dieffenbach*, "scoundrels" and "villains" stole plaintiffs' names and account data through compromised PIN pads at a national retailer. The named plaintiff alleged that she suffered actual injury even though her bank refunded all fraudulent charges in less than three days. The court agreed, not because of unreimbursed fraudulent charges or allegations that identity theft might occur in the future but rather because "the data theft may have led [the plaintiffs] to pay money for credit-monitoring services, because unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal, and because the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective."

In other words, allegations of the rather abstract concept of the lost time value of relatively small sums money for less than three days can now be considered actual injury for purposes of standing in data breach cases.

In re Zappos.com, Inc.

The Zappos breach in 2012 spawned several class actions that were consolidated for pretrial proceedings. While some plaintiffs alleged the hackers used stolen information to conduct subsequent financial transactions, the

particular motion to dismiss before the Ninth Circuit in *In re Zappos.com, Inc.* concerned claims from plaintiffs "based on the hacking incident itself, not any subsequent illegal activity." In finding standing for these plaintiffs, the Ninth Circuit did not focus on the injury itself but rather on the type of information stolen (credit card numbers, names, emails and contact information), noting "the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming.'"

While the holding in *Zappos.com* is not particularly remarkable as its keeping with the trend, part of the court's rationale for finding standing was striking. Courts usually differentiate between the claims of plaintiffs who allege actual injury versus those who allege an increased risk of future injury. For example, back in 2017 in *In re Supervalu, Inc.*, the Eighth Circuit dismissed as speculative the claims of the plaintiffs who did not allege any misuse of their personal information, but allowed the claim of the single plaintiff who alleged actual misuse (even though the injury was de minimis).

But in *Zappos*, the Ninth Circuit examined the allegations of all plaintiffs holistically. Even though the motion to dismiss did not relate to the plaintiffs alleging actual injury, the court used the allegations of actual injury by these plaintiffs (such as specific fraudulent charges or incidents of identity theft) to support the standing arguments of those plaintiffs who did not. In the court's view, the fact that some plaintiffs suffered the actual injury of identity theft stemming from the breach showed that the plaintiffs who had not yet suffered such injury nevertheless faced an increased risk of such injury. The court also considered non-financial harm (the fact that two plaintiffs lost control of their AOL email accounts and spam advertisements were sent to people in their address books) as "further support" that the information the hackers accessed was of the type that is used to commit identity fraud or theft.

It remains to be seen if other courts will adopt similar approaches.

See "Minimizing Class Action Risk in Breach Response" (Jun. 8, 2016).

Some Courts Remain Skeptical

Despite this trend, some courts remain skeptical of anything outside of allegations of actual damage or misuse. For example, the Fourth Circuit found standing for data breach plaintiffs in *Hutton v. National Board of Examiners in Optometry Inc.* But in so doing, the court re-affirmed its 2017 opinion in *Beck v. McDonald*, and kept the focus on whether the plaintiffs alleged actual injury stemming from the data breach.

Hutton presents a unique factual predicate. In July 2016, optometrists from across the United States discovered that Chase Amazon Visa credit card accounts had been fraudulently opened in their names. After discussing the issue in social media forums dedicated to optometrists, the victims realized a potential common link: (1) the fraudulent accounts could not have been opened without the use of their respective Social Security numbers and dates of birth; and (2) all victims had given this data to the defendant upon graduation from school when sitting for board-certifying exams. In response to these allegations on social media, the defendant published statements that it

was investigating the issue. However, the defendant never confirmed or admitted that a breach or unauthorized access to the victims' personal information ever occurred.

In finding standing, the Fourth Circuit first re-affirmed its holding in *Beck*: "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." Thus, "a plaintiff fails to establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it." However, in the context of *Hutton*, the court found "Plaintiffs have been concretely injured by the data breach because the fraudsters used–and attempted to use – the Plaintiffs' personal information to open Chase Amazon Visa credit card accounts without their knowledge or approval." Thus, there was "no need to speculate" that plaintiffs had been injured.

The 2018 *In Re Supervalu Inc.* decision further illustrates the types of allegations which still may fall short of Article III standing. This particular opinion was the latest in a long line of decisions from both the United States District Court of Minnesota and the Eighth Circuit relating to the breach of payment systems at several grocery store chains. In this iteration, plaintiffs who had already been dismissed for lack of standing sought to amend their complaint to add allegations "related to the increased risk of harm" plaintiffs suffered as a result of the breach. Specifically, the plaintiffs sought to add general allegations that "three credit union officers have reported that some payment cards issued by their institutions were compromised in the data breach, and that some accounts incurred fraudulent charges." They also sought to add allegations from industry reports stating 40 percent of those whose card numbers were compromised in a particular year subsequently became fraud victims.

The court found these allegations did not cure the standing deficiencies. The allegations from the credit union officers had previously been considered and rejected as none were tied specifically to a named plaintiff. With respect to the industry reports, the court found these did not "demonstrate a substantial risk" of future fraud since they showed only a 40-percent chance of fraud, meaning "the majority of consumers whose payment cards are compromised in a breach will not become fraud victims as a result of the breach." It should be noted that no other courts have yet articulated such a strict standard for what percentage likelihood constitutes a "substantial risk" of future injury.

Staying in the mid-west, the United States District Court for the Northern District of Illinois decided *CS Wang & Associate v. Wells Fargo Bank, N.A.* While not a data breach case, it is still instructive of the types of hypothetical injuries that courts reject for standing purposes post-*Spokeo*. Here, the plaintiffs alleged violation of the California Invasion of Privacy Act through the secret recording of telemarketing calls. Plaintiffs claimed they suffered two injuries as a result of the non-consensual recordings: (1) a violation of privacy that is itself an injury; and (2) "that subsequently sharing and storing the recordings on cloud-based computer systems created a risk of a data breach." While the court ultimately found there was standing for the violation of privacy, it expressly rejected any standing based "a risk of data breach," noting this 'highly attenuated chain of possibilities does not satisfy the requirement that threatening injury must be certainly impending."

The *Frank v. Gaos* Supreme Court Wild Card

The Supreme Court will tackle significant issues in *Frank v. Gaos*. The case involves something called the HTTP referrer header – essentially a code used in internet traffic that tells a target website some limited information about how that particular internet user arrived at the target website. Specifically, the plaintiffs alleged that Google's practice of including information about a user's search terms in the HTTP referrer header violated the Electronic Communications Privacy Act and the Stored Communications Act.

The plaintiffs argued that that information disclosed in the HTTP referrer header triggered a violation of privacy, even though it does not directly identify the user. The primary standing question is whether there is a sufficient risk of re-identification based on the HTTP referrer headers such that there is a concrete injury for Article III standing purposes.

It is possible that the Supreme Court decides to resolve this case without addressing the standing issue. However, any pronouncements regarding standing could either set in stone or fundamentally alter the current trend towards a lower bar for Article III standing in data breach and privacy cases. Thus, this pending opinion is a significant unknown that should be closely monitored in the coming weeks and months.

See also "Implications of the Supreme Court's Carpenter Decision on the Treatment of Cellphone Location Records" (Jul. 25, 2018).

Breach Litigation Thriving

These cases are clear signals to all potential defendants that breach litigation will not die quickly.

In the just over two short years since *Spokeo*, the majority of federal appellate circuits have lowered the bar for data breach plaintiffs to show injury-in-fact and Article III standing. It is safe to say this is not just a possible trend towards lower standing requirements but rather the new reality. How then should companies respond or change their approaches to data breach preparation and litigation?

1) Prepare for Longer, More Costly Litigation With Multiple Phases

Budgeting for a crisis is never easy, but, as the recent Marriott breach illustrates, the stakes are too high to ignore. It is reported that Marriot could face total costs of up to $1 billion for a breach that affected an estimated 500 million guests. Thus, if it is more difficult to quickly dismiss claims from data breach plaintiffs based on standing, then the inevitable outcome is longer litigations that will use a greater percentage of your litigation budget over longer periods of time. This, in turn, increases the long-term financial impact of a breach to your company. The cases cited above are further cautionary examples.

The breaches in *Dieffenbach*, *Zappos*, and *In re Supervalu* all occurred back in 2012 and 2014. Now, after years of expensive motions practice and federal appeals, some of these defendants are still faced with class actions, fact and expert discovery, substantive fights on the merits of the cases and possible jury trials.
See also "Defense and Plaintiff Perspectives on How to Survive Data Privacy Collateral Litigation" (Mar. 8, 2017).

2) Shift the Focus of Motions to Dismiss From Standing to Failure to State a Claim

Even when they can show standing, data breach plaintiffs may continue to have difficulty in articulating an appropriate legal claim. For example, courts may find that straight negligence claims are barred by the economic loss doctrine (as did the court in *In re Supervalu*). And the 7th Circuit in *Dieffenbach* also opened the door for defendants to raise the argument that they are equally victims of the data thieves such that "plaintiffs may have a difficult task of showing an entitlement [under state law] to collect damages from a fellow victim of data thieves."

Lastly, even though courts use it as an injury for purposes of standing as they did in *Dieffenbach*, state law may not actually support finding damages for liability based on lost personal time.

This issue – whether lost-time damages for lost personal time are recoverable for state law claims–was discussed in great length and detail outside of the data breach context in *In re: General Motors LLC Ignition Switch Litigation*. The court concluded that, while consumers could recover lost-time damages where lost time was understood as lost earnings or its equivalent, the overwhelming majority of states did not allow such damages where it was understood as lost personal time. Thus, Defendants still have opportunities to bring motions to dismiss for failure to state a claim under Federal Rule 12(b)(6). However, as more states pass laws creating private rights of action for data breaches, the ability to dismiss for failure to state a claim will also decrease.

See, *e.g.*, "Understanding the Potential Implications of Pennsylvania's Newly Recognized Common Law Duty to Protect Personal Information" (Dec. 12, 2018).

3) Double-Check Internal Processes and Procedures

Use this time at the start of the year to revisit internal systems and policies. Compliance is a critical part of any privacy and security regime, but this pre-breach work must be done with an awareness of its impact on litigation strategy and likelihood of success during litigation.

Similarly, an incident response plan cannot be a purely technical document geared towards engineers but rather should be the company-wide script for any incident that seamlessly integrates in-house and outside counsel, forensics, public relations and executive management into the response plan. This often means involving outside litigation counsel in the compliance and planning picture to ensure that the potential litigation pitfalls are considered, analyzed and planned for in advance.

See also "Checklist for an Effective Incident Response Plan" (Jul. 20, 2016).

Jon Knight (CIPP/US, CIPP/E, CIPM) is a litigator at Boies Schiller Flexner who advises clients on a variety of technology-focused issues including data privacy and security, breach response, regulatory compliance and intellectual property disputes.