2021 was another year of high activity in the realm of data event and cybersecurity litigations with several noteworthy developments. CPW has been tracking these cases throughout the year. Read on for key trends and what to expect going into the 2022.

Recap of Data Breach and Cybersecurity Litigations in 2020

2021 heralded several developments in data breach and cybersecurity litigations that may reshape the privacy landscape in the years to come. However, in many ways 2021 litigation trends were congruent with the year prior. Before delving into where we may be headed for this important area of data privacy litigation in 2022, let's do a short recap of where we were at the end of 2020.

Recall that the number of data events in 2020 was more than double that of 2019, with industries that were frequent targets of cyberattacks including government, healthcare, retail and technology. In this instance, correlation equaled causation—as more entities experienced crippling security breaches, the number of data breach litigations filed also increased. There were three trends that marked the cybersecurity landscape that we covered in CPW’s 2020 Year in Review:

First, in 2020 plaintiffs bringing data breach litigations continued to rely on common law causes of action (negligence and fraud, among others) in addition to asserting new statutory claims (although of course there were exceptions). Challenges to a plaintiff’s Article III standing in the wake of a data event were pervasive, with defendants arguing that allegations of future speculative harm were inadequate to establish federal subject matter jurisdiction.

Second, in spring 2020, a federal court ordered production of a forensic report prepared by a cybersecurity firm in the wake of a data breach. The report was found not protected as attorney work product despite having been prepared at the direction of outside counsel. Commentators at the
time wondered if this was a harbinger of future rulings regarding privilege in the context of privacy litigations.

And **third**, there were several warning signs that the legal fallout from a data breach can extend to company executives and the board. As just one instance, in 2020 a company’s former Chief Security Officer (CSO) was charged with obstruction of justice and misprision of felony for allegedly trying to conceal from federal investigators a cyberattack that occurred in 2016, exposing the data of 57 million individuals.

Perhaps unsurprisingly, these earlier trends signaled in part what was on the horizon in 2021 as discussed in greater detail below.

**Article III Standing in Cybersecurity Class Action Litigations**

The past several years have seen a not-so-quiet revolution in standing jurisprudence, and 2021 was no different. Standing under Article III of the U.S. Constitution, in the Supreme Court’s oft-repeated phrasing, is an “irreducible constitutional minimum” requiring that a party be able to demonstrate: (1) an injury in fact; (2) that the injury was caused by defendant’s conduct; and (3) that the injury can likely be redressed by a favorable judicial decision.

The standing issue that defined 2021 was “speculative future harm.” In February, the Eleventh Circuit highlighted a long-running circuit split regarding whether plaintiffs had standing to assert claims based solely on the disclosure of their information couples with an increased risk of future harm. In *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021), the court found that standing required a concrete and particularized injury that was actual or imminent. The *Tsao* plaintiff based his injuries on fear of future harm, as well as preemptive steps taken to ward off potential identity theft. In line with the majority of circuits to have addressed the issue, the court found that none of these potential injuries conferred standing.


In the midst of this growing chorus of cases rejecting speculative future harm as a basis for standing came the Second Circuit, which issued a massive opinion trying to harmonize years of precedent both finding and rejecting standing. *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 297 (2d Cir. 2021) held that, in the abstract, a plaintiff could establish standing based on a substantial risk of identity theft or fraud, but that such an argument would be fact and case-specific.
Then came June’s Ramirez v. Transunion, 141 S. Ct. 2190, in which the Supreme Court revisited the question of what constitutes an “injury in fact” in the data breach context. The Ramirez class consisted of affected individuals who, in the main, alleged only that inaccurate information existed on their credit files, with no corresponding dissemination to a third party or any harm resulting from that dissemination. The Supreme Court determined that where the vast majority of a putative class suffered no actual injury, let alone the type of injury suffered by a class representative, no standing existed. The Supreme Court also determined that “the mere risk of future harm, without more, cannot qualify as a concrete harm in a suit for damages.”

On a related note, while commentators worried that Ramirez would preclude data breach litigations from being brought in federal courts, such concerns have not yet materialized. The courts in Blackbaud and Cotter v. Checkers Drive-In Restaurants, Inc., 2021 U.S. Dist. LEXIS 160592 (M.D. Fla. Aug. 25, 2021), distinguished Ramirez on procedural grounds. Meanwhile, some courts have indicated that an impending injury or substantial risk could suffice for injury in fact in data breach litigation. The court in Griffey v. Magellan Health Inc., 2021 U.S. Dist. LEXIS 184591 (D. Az. Sep. 27, 2021), found that plaintiffs alleged risks of future harm that were “certainly impending” and thus had standing. All in all, however, pleading a data incident without something more probably does not survive a motion to dismiss. That’s what happened in Legg v. Leaders Life Ins. Co., 2021 U.S. Dist. LEXIS 232833 (W.D. Okla. Dec. 6, 2021), where plaintiffs’ allegations of general risks of harm did not suffice.

Ramirez has also led to consideration of timing and cause-and-effect in data privacy litigation, with courts focusing not only on the existence of concrete harm, but whether the harm could have actually been caused by the breach itself. The Eastern District of Missouri determined in Mackey v. Belden, Inc., 2021 U.S. Dist. LEXIS 145000 (E.D. Mo. Aug. 3, 2021) that the theft of a Social Security number, coupled with the filing of a false tax return after the theft occurred, was sufficient to confer standing, while the Central District of California determined in Burns v. Mammoth Media, Inc., 2021 U.S. Dist. LEXIS 149190 (C.D. Cal. Aug. 6, 2021) that standing requires a plaintiff show an actual connection between his or her damages and the breach, rather than simply speculating that any purported harm that occurred must have been the result of the breach.

Discovery Disputes Over Work Product and Attorney Client Privilege


If you recall, the Capital One decision involved a motion to compel a report on a data breach prepared by Capital One’s pre-established security consultant. Capital One, 2020 U.S. Dist. LEXIS 91736, at *12. This was probably Capitol One’s biggest mistake: This “long-standing” business
relationship became the key dispositive liability for keeping that report protected under the work product doctrine. Id. The court in Capital One scrutinized that business relationship as well as prior reports prepared for cybersecurity purposes and, as a result, ascertained that the consultant’s report would have been prepared in a similar form regardless of the litigation. Thus, the report did not meet the “because of” litigation standard for work product protection. Presumably because of the preexisting relationship, that decision did not need to address the narrow Kovel test for whether the report would be protected under the attorney-client privilege as work essentially prepared by the litigation counsel’s expert or paralegal.

Relying on the Capital One decision, a D.C. district court decided Clark Hill earlier this year. Clark Hill involved a cybersecurity attack directed at a law firm. In attempting to avoid production of the breach report, Clark Hill sought to rely on the work product doctrine arguing that the report they sought to withhold was created “because of” anticipated litigation. Clark Hill, PLC, 338 F.R.D. at 10. Rather than simply assert that, given that case law exists noting that incident response reports serve business functions as well, Clark Hill attempted to make a more nuanced argument. Specifically, Clark Hill argued, relying on a concept first introduced by In re Target, that two reports existed; one which was prepared for litigation and the other of which was to be used to address security concerns. That distinction, while accepted by the Court, failed Clark Hill because their other report was nowhere near as substantive, was not described in the interrogatory responses as a basis for their response, and the report Plaintiff sought had been circulated outside of the circle of employees and lawyers who needed to know about it for the litigation. Id. at 12. Clark Hill similarly lost on the attorney-client privilege because, in attempting to invoke the Kovel Doctrine. Clark Hill failed to meet the criteria of this test because the numerous security improvement recommendations in the breach report at issue demonstrated that the report was not prepared by an expert advising litigators on how to provide legal advice but was rather the result of independent vendors working to cure a business issue – Clark Hill’s cybersecurity deficiencies. Clark Hill, PLC, 338 F.R.D. at 11.

Issued this summer, In Re Rutter is the third federal court decision addressing these issues. While Clark Hill cited Capital One in its analysis, In Re Rutter’s presents an independent analysis and arrives at the same conclusion. The potential data breach at issue in In Re Rutter’s concerned payment card information at the point-of-sale (POS) devices used by defendants. Rutter’s received two alerts on May 29, 2019, which “detail[ed] the execution of suspicious scripts and indications of the use of potentially compromised credentials.” In response, Rutter’s hired outside counsel, BakerHostetler, “to advise Rutter’s on any potential notification obligations.” BakerHostetler in turn hired a third party security firm “to conduct forensic analyses on Rutter’s card environment and determine the character and scope of the incident.” In re Rutter’s Data Sec. Breach Litig., 2021 U.S. Dist. LEXIS 136220, at *3.

Plaintiffs in In Re Rutter’s learned about the defendant’s investigation and resulting report during the Fed. R. Civ. P. 30(b)(6) deposition of Rutter’s ill-prepared Vice President of Technology. Following that deposition and as a result of the deponents framing of the process underlying the report, Plaintiffs sought production of the security firm’s written report and related communications. Rutter’s objected, citing the work product doctrine and attorney-client privilege. Applying the general work product doctrine precedent described above, the court held that the work product doctrine did not protect the security firm’s report and related communications from disclosure in discovery largely because of how that report was characterized at deposition as indistinct from a factual report prepared without involvement of counsel.

Thus, both Clark Hill and In Re Rutter’s serve as sobering reminders that while reports prepared for and at the request of counsel in anticipation of litigation can be privileged, compliance officers and
counsel must scrupulously avoid blurring the lines between “ordinary course” factual reports and reports genuinely prepared for assisting trial counsel. In re Rutter’s also serves as a reminder that preparing 30(b)(6) witnesses can be critical as their testimony can be highly significant, if not dispositive, for a court when assessing assertions of privilege.

These two new cases further cement the widespread implications from Capitol One for both data privacy litigation strategy. All three cases pose lessons for litigators and incident response counsel on the appropriate framing of incident response efforts before and during litigation. For more a more in depth analysis of the facts underlying these cases and the take-away lessons from them, see our earlier publication here.

**Plaintiff-Side Developments**

Data breach litigations continued to be filed at a brisk pace in 2021 in industries ranging from ecommerce, finance, mortgage providers, technology, and software cloud companies to healthcare, wellness, retail, and fast-food, among others.

Many of these litigations were dismissed at the pleadings stage, either for lack of Article III standing (discussed above) or for failure to plead a cognizable claim. These cases reiterate that merely alleging that a data event or cyberattack occurred, without more, does not mean that plaintiffs automatically can go forward with a case. Conclusory, ipse dixit allegations are not sufficient. Plaintiffs are taking note of these decisions and increasingly relying on a blunderbuss pleading strategy (by raising multiple statutory and common law claims in a single complaint) in an effort to have their claims survive a motion to dismiss.

However, because plaintiffs (particularly those that allege merely speculative future harm as a result of a data event) have difficulty establishing the core elements of causation and damages, these efforts have met with mixed success. Mere alleged misappropriation of personal information may not suffice for purposes of establishing a plaintiff’s damages.

Of course, it goes without saying that class action plaintiffs have also taken an expansive pleading strategy in the hopes that they will be able to cobble together a claim under one of the state or federal privacy statutes that provides for liquidated statutory damages upon establishment of a violation (the California Consumer Privacy Act (“CCPA”) and federal Driver’s Privacy Protection Act were two frequent targets).

**Other Trends: Emergence of the Data Breach Consumer Pricing Dispute and a Decline in MDLs**

Additionally, 2021 also saw the first instance in which a data event litigation was framed as a quintessential consumer pricing dispute—perhaps signaling that such cases may become more common. In the wake of a ransomware attack involving the Colonial Pipeline, two groups of Plaintiffs filed suit alleging that the owners of the Colonial Pipeline failed “to properly secure the Colonial Pipeline’s critical infrastructure – leaving it subjected to potential ransomware attacks like the one that took place on May 7, 2021.” See Dickerson v. CDCP Colonial Partners, L.P., Case No. 1:21-cv-02098 (N.D. Ga.); EZ Mart 1, LLC v. Colonial Pipeline Company, Case No. 1:21-cv-02522 (N.D. Ga.). This included the assertion that Defendants “failed to implement and maintain reasonable security measures, procedures, and practices appropriate to the nature and scope of [Defendants’ business operations].” Plaintiffs sought to the Complaint seek to certify a nationwide
class consisting of "[a]ll entities and natural persons who purchased gasoline from May 7, 2021 through Present and who paid higher prices for gasoline as a result of the Defendant’s conduct alleged herein (hereinafter the “Class”).” Will we see more of this going forward? Time will tell.

Finally, although the Judicial Panel on Multidistrict Litigation (“JPML”) recently transferred and centralized over 40 data event and cybersecurity class actions brought against T-Mobile in the Western District of Missouri, data breach multidistrict litigations (“MDLs”) declined over prior years. There were several instances in which the JPML declined requests to consolidate and coordinate pretrial proceedings in the wake of a data event. Justifications given by the JPML in declining consolidation this year included that “centralization under Section 1407 should be the last solution after considered review of all other options,” which include “agreeing to proceed in a single forum via Section 1404 transfer of the cases and voluntary cooperation and coordination among the parties and the involved courts to avoid duplicative discovery or inconsistent rulings.” When cybersecurity litigations have been primarily filed in the same forum or the parties are already coordinating, the JPML especially was disinclined to order MDL formation in 2021.

Looking Forward

In many regards, 2021 demonstrated the axiom “the more things change, the more they stay the same.” Cybersecurity litigation trends in 2021 were a continuation of 2020. Article III standing, privilege considerations and novel pleading strategies used by plaintiffs to survive a well-crafted motion to dismiss are expected to remain key issues in data event litigations in 2022. Additionally, a larger development on the horizon remains the specter of liability to corporate officers and the board in the wake of a widespread cyberattack. While the majority of cybersecurity litigations filed continue to be brought on behalf of plaintiffs whose personal information was purportedly disclosed, shareholders will increasingly look to hold executives responsible for failing to adopt reasonable security measures to prevent cyberattacks in the first instance.

Needless to say, 2022 should be another interesting year for data event litigations and for data privacy litigations more broadly. Not to worry, CPW will be there to keep you in the loop. Stay tuned.

© Copyright 2024 Squire Patton Boggs (US) LLP

National Law Review, Volumness XI, Number 357

Source URL: https://www.natlawreview.com/article/2021-year-review-data-breach-and-cybersecurity-litigations