LAW FIRM "MOST FEARED" GLOBALLY BY LARGE BUSINESSES
BTI Consulting Group Survey

January 2023

quinn emanuel

quinn emanuel urquhart & sullivan, llp | business litigation report

atlanta | austin | berlin | boston | brussels | chicago | dallas | doha | hamburg | hong kong | houston | london | los angeles | mannheim | miami | munich
neuilly-la defense | new york | paris | perth | riyadh | salt lake city | san francisco | seattle | shanghai | silicon valley | stuttgart | sydney | tokyo | washington, d.c. | zurich

Private Data Breach Litigation Comes of Age

Overview

Data breaches are everyday occurrences and major high-profile breaches are becoming more common. In the past three years, industry-leading companies such as Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Meta/Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020) have all experienced significant breach events. Given the prevalence of remote working, the shift to cloud-based storage, and the ever-increasing sophistication of cybercriminals, data security risk is not going away.

Data breaches produce immense financial aftershocks for targeted companies. In 2022, the average cost of a data breach for U.S. companies reached a record high—$9.44 million. *See Cost of a Data Breach Report 2022* at 9-10, IBM (July 2022), https://www.ibm.com/reports/data-breach. Given that 83% of organizations have now suffered more than one data breach, the prospect of a business facing reoccurring costs in this area is a virtual certainty. *Id.* at 4, 6. But companies also face fiscal consequences that go well beyond the technical cost of redressing the breach, possible reputational harm to their brands, and potential declines in share price. Sixty percent of businesses have been compelled to increase the price of their services or products because of a data breach. *Id.* at 5. Costly regulatory action is also likely to follow. For instance, following its 2017 data breach (which affected almost 150 million Americans), Equifax faced litigation brought by 48 states, as well as the District of Columbia and Puerto Rico, which it settled for $175 million, and an enforcement action pursued by the Consumer Financial Protection Bureau, which it resolved for $100 million in civil penalties. *See Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FTC Press Release (July 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach.

Companies face yet another major risk after a

(continued on page 2)

INSIDE

Quinn Emanuel Urquhart & Sullivan, LLP Welcomes New Partner Class page 16

Former SEC Official C. Dabney O'Riordan Joins the Firm as a Partner, Based in Los Angeles and Washington, D.C.

Dabney O'Riordan has joined the firm as a partner based in the firm's Los Angeles and Washington, D.C. Offices. Dabney, a more than seventeen-year veteran of the SEC, is a pre-eminent expert in enforcement, regulatory, and compliance oversight of asset managers. Prior to joining the firm, Dabney was the longest-serving leader of the SEC Enforcement Division's Asset Management Unit (AMU), a nationwide unit of approximately 60 lawyers and industry experts that leads the SEC's efforts to investigate and litigate issues involving the asset management industry. Beyond overseeing hundreds of investigations conducted by staff across the country, Dabney led the Enforcement Division's efforts to address emerging issues in the asset management industry, including as a founding member of the Division's Climate and ESG Task Force, and worked closely with other SEC leaders on related rules, guidance, and examination priorities. Q

data breach—one which is increasing exponentially—data breach litigation brought by private plaintiffs, often in the form of class actions brought by sophisticated plaintiffs' counsel who specialize in such cases. Private civil litigation is now a probability, not a possibility, after a major data breach. 36 major data breach class actions were filed in 2021, a 44% increase from 2020. Private plaintiffs typically race to the courthouse to jockey for position, with complaints now brought on average within four weeks of a breach announcement.

These private actions, had they been pursued a decade earlier, would have faced little prospect of success. Private plaintiffs during the initial wave of data breach litigation struggled to establish standing or successfully plead duty, causation, and damages *See, e.g.*, *In re: Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1212 (N.D. Cal. 2014) (noting that "courts in data breach cases regularly" dismiss claims because "increased risk of future harm is insufficient to confer Article III standing"); *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 963-65 (S.D. Cal. 2014) (dismissing negligence claims because "Plaintiffs' allegations of causation and harm are wholly conclusory" and Plaintiffs "failed to allege a single cognizable injury proximately caused by Sony's resulting breach"). Their task was complicated by facts that, by their nature, often involve incremental risk and latent harm. In the intervening years, however, the plaintiffs' bar has developed a series of creative theories that have frequently succeeded in moving data breach actions beyond the pleadings stage. The result is that large settlements of consumer data breach cases are now quite common, with notable recent resolutions involving T-Mobile ($350 million to consumers), Equifax ($380.5 million), Capital One ($190 million), Zoom ($85 million), Hy-Vee ($20 million), and Home Depot ($12.88 million).

This article explores the latest developments in private data breach litigation. We focus first on the challenges that plaintiffs face in establishing standing and damages. The assessment of whether these plaintiffs have suffered a cognizable injury-in-fact (as required for Article III standing) is necessarily intertwined with the type and viability of the harms they allege. Accordingly, we first consider both standing and damages. We then analyze the state-of-the-art claims currently being asserted by plaintiffs and the defenses being deployed by companies in response. Finally, we conclude with a discussion of expected future trends.

Standing and Damages – A Key, Unsettled Battleground

Defendants typically contest the standing of data breach plaintiffs at the pleadings stage, and usually do so on two grounds: (1) failure to establish a concrete and particularized injury-in-fact; and (2) failure to adequately allege a causal connection between their alleged injuries and the defendant's conduct. In recent years, defendants' causation arguments have met with little success. The resolution of a causation challenge often involves issues of fact inappropriate for resolution on a motion to dismiss. In addition, most plaintiffs can overcome traceability concerns created by the participation of a third party (*i.e.*, the hacker) by alleging a clear series of actions and omissions by the defendant company, such as poor data security practices or deficient oversight, that are sufficient to establish a nonspeculative causal link.

As a result, the real action at the pleadings stage lies in the first category—*i.e.*, injury-in-fact. As the U.S. Supreme Court explained in *Spokeo, Inc. v. Robins*, "Article III standing requires a concrete injury even in the context of a statutory violation," and courts must assess whether the plaintiffs' alleged injury has a "close relationship" to a harm "traditionally" recognized as providing a basis for a lawsuit in American courts. 578 U.S. 330, 341 (2016). With respect to injunctive relief, "a person exposed to the risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210 (2021) (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). But "a plaintiff's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages"—which is one of the most critical issues to the plaintiffs' bar in bringing data breach class actions. *Id.* The injunctive relief sought by the data breach plaintiffs' bar remains an important consideration, both for plaintiffs and defendant-companies. Data breach plaintiffs tend to plead the prescriptive relief they seek with great specificity and often include demands that the defendant routinely test its employees on security measures and engage independent third-party security auditors. *See, e.g.*, *Marlowe v. Overby-Seawell Co.*, No. 1:22-mi-99999, ECF Doc. # 2851, Complaint (Prayer for Relief) ¶ C(i)-(xvi) (N.D. Ga. Sept. 9, 2022).

It is necessary to understand who is impacted by a data breach, and in what ways, to fully comprehend the current injury-in-fact standing battle between plaintiffs and defendant companies as it relates to a *damages* class. Following a data breach, the consumers, users, employees, or patients of the targeted entity usually fall within three broad categories:

a. <u>Group One – Plaintiffs Who Have Experienced Direct Economic Injuries</u>

First, there is some portion of the group that has suffered direct economic damage resulting from misuse of their Personal Information (PI) or Protected Health

Information (PHI) stolen in the data breach ("Group One"). Common injuries of this type include fraudulent charges on credit cards, fraudulent withdrawals from bank accounts, and the cost of any measures taken to resolve these fraudulent transactions—including time invested and money spent on combating and mitigating these manifestations of identity theft. Private data breach plaintiffs routinely seek actual and consequential damages connected to these economic losses, out-of-pocket expenditures, and time spent addressing the aftereffects of these harms.

Courts now routinely find that Group One plaintiffs meet the "injury-in-fact" or "concrete-harm" requirement for Article III standing. *See Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2013) (finding concrete injury because party suffered actual harm in the form of identity theft and credit card fraud). It is well settled that a "monetary harm," such as an out-of-pocket loss, falls within the "traditional tangible harms" required for standing. *TransUnion*, 141 S. Ct. at 2204. The same is true even where the losses suffered by this group have been reimbursed, "since they have suffered the actionable intangible harm of the wrongful use and dissemination of their private information, like the interests protected by common law privacy torts." *In re: Am. Med. Collection Agency, Inc. Consumer Data Sec. Breach Litig.*, 2021 WL 5937742, at *8 (D.N.J. Dec. 16, 2021) (citing *TransUnion*, 141 S. Ct. at 2208). Courts have also consistently recognized plausible economic injuries stemming from any prophylactic or remedial expenses incurred by Group One plaintiffs, reasoning that, because an actual harm has already "materialized," these "injuries" are no longer speculative or based on an uncorroborated fear of future theft. *See Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164-67 (1st Cir. 2011) ("cost of credit monitoring services and identity theft insurance" are cognizable injuries when incurred by plaintiffs who had already suffered fraudulent charges); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 623-24 (D.N.J. 2014) (similar); *Hutton*, 892 F.3d at 622 (same).

b. Group Two – Plaintiffs Who Can Show That Their Personal Information Was Accessed

There is another segment of the affected population whose members have not experienced direct economic harm, but who have experienced events suggesting that their PI or PHI may have been wrongly accessed and distributed ("Group Two"). These individuals may have witnessed foiled attempts at identity theft, unsuccessful fraudulent charges, a marked increase in scam phone calls or spam emails, or the appearance for sale of their PI on the dark web. While the experiences of these plaintiffs differ, they have some corroboration that their PI or PHI was accessed.

Although slightly more controversial than Group One, courts now frequently find that such Group Two plaintiffs have pleaded "intangible harms" that are sufficiently "concrete" to establish standing—particularly given the U.S. Supreme Court's 2021 decision in *TransUnion v. Ramirez*, which identified "disclosure of private information" and "intrusion upon seclusion" as traditionally actionable "intangible harms." *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *9; *TransUnion*, 141 S. Ct. at 2204 (listing traditional intangible harms). While cognizable for the purposes of standing (and thus preserving this group as members of a potential damages class), intangible harms like increased spam emails or foiled fraudulent charges do not usually require extensive monetary compensation. As such, private plaintiffs often seek nominal—or, where available, statutory—damages for these types of injuries.

c. Group Three – Plaintiffs Whose Personal Information Was Stored on the Compromised Systems—New Damages Theories

The remaining consumers, users, employees, or patients had PI or PHI stored on the compromised systems but may not have a firm indication that their data was accessed, downloaded, or misused by an unauthorized party ("Group Three"). This group faces the biggest hurdle in meeting the "concrete-harm" standard required for Article III standing.

The plaintiffs' bar has focused its efforts on Group Three to try to maximize leverage and preserve these affected individuals as viable plaintiffs. Their pursuit of more exotic theories to support injury-in-fact for this category of plaintiffs also allows them to allege a wider array of damages incurred by Groups One and Two, as the additional "harms" identified will also apply to members of those groups. Below are examples of how private plaintiffs articulate the injuries and damages they are pursuing to achieve these ends:

1. To the extent that plaintiffs now face a reduced credit score due to the breach (which increases the cost of borrowing, insurance, and deposits and makes difficult the ability to secure more favorable rates), plaintiffs have been harmed and compensatory damages are owed. Similarly, to the extent that plaintiffs lost the use of or access to their credit, accounts, and/or funds for a period due to the data breach, they should be compensated for that harm in the form of compensatory or nominal damages.
2. Plaintiffs have been injured because they face a real and substantial risk of future identity theft. Their PI was present on a system that was compromised by a

cybercriminal, and the fact that the PI of others on that same system has been accessed and misused makes real and imminent the increased risk of identity theft faced by those who have yet to experience misuse. At the very least, nominal damages are owed for this heightened danger

3. Considering this imminent, immediate, and continued risk of identity theft and identity fraud, this group should be awarded compensatory damages like Groups One and Two for any time, effort, and expenses incurred in undertaking mitigation efforts to guard against future identity theft and fraud, such as reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. Some plaintiffs have even pushed for compensation for "lost opportunity costs" connected to the time they spent researching how to prevent, detect, contest, and recover from fraud and identity theft.
4. PI or PHI has real economic value. Advertisers pay money to access PI so that they may bolster the effectiveness of their outreach, and companies frequently offer incentives so that customers share PI with them. The value of PI and PHI can be quantified by reference to established rates for this information, including by showing what PI and PHI sells for on the black market or dark web. The compromise and unauthorized publication of plaintiffs' PI and/or PHI reduces its value. This harm should be redressed through the payment of compensatory damages reflecting the resulting diminution in value.
5. The defendant's deficient security, which allowed the breach to occur, means that plaintiffs were robbed of the "benefit of the bargain" in transacting with the defendant. Every year, the defendant spends a certain portion of its budget on data security. The defendant passes on that expenditure to customers such that a certain percentage of the money paid by plaintiffs in return for the defendant's services is to ensure adequate protection for their PI. The breach indicates that the defendant was not upholding this portion of the bargain. Plaintiffs have been harmed by this lost benefit and are owed compensatory damages tied to the percentage of their payments to the defendant that went to substandard data security. At the very least, nominal damages are owed for this injury.
6. Plaintiffs were injured because they overpaid for the defendant's products or services. The data breach indicates that the defendant had inadequate data security. Had the defendant's inadequate security been publicly known, it would have decreased demand for its goods or services, which would have resulted in lower prices paid by consumers for its goods or services. Consequently, plaintiffs overpaid for the defendant's goods or services and are owed compensatory—or, at the very, nominal—damages resulting from this harm. The court in *In re: Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 341 F.R.D. 128 (D. Md. 2022), recently certified a data breach class based on this overpayment theory.
7. Plaintiffs experienced a trespass, as their PI or PHI was subjected to an unauthorized incursion. As a result of this invasion of privacy, plaintiffs have experienced emotional distress—a harm for which they should be provided compensatory (or nominal) damages.

d. Confusion Remains – Particularly with Respect to the More Creative Harms Alleged

Federal law regarding the type of standing and damages arguments advocated by Group Three plaintiffs and identified above remains highly unsettled. Small differences in the facts pleaded or the individual preferences of the court are often outcome-determinative.

For instance, in *McMorris v. Carlos Lopez & Assocs., LLC*, decided in April 2021, the Second Circuit appeared to take a significant step towards recognizing standing for this group of plaintiffs. It explicitly held that "plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data." 995 F.3d 295, 301 (2d Cir. 2021). It then listed three "non-exhaustive factors" to be considered by courts when weighing whether data breach plaintiffs have adequately alleged an Article III injury-in-fact based on an "increased risk" theory: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Id.* at 303. However, acceptance of the view that plaintiffs who have not yet experienced identity theft could have standing still varied between jurisdictions. Generally, "the Sixth, Seventh, and Ninth Circuits ha[d] accepted that 'an increased risk of identity theft *is* sufficient to establish injury-in-fact,' while in contrast, the First and Third Circuits found that an increased risk of identity theft *did not* constitute injury-in-fact." *In re: Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 524-25 (M.D. Pa. 2021) (quotation marks and internal citations omitted). *Compare In re: Zappos.com, Inc.*, 888 F.3d 1020, 1027-28 & n.7 (9th Cir. 2018) (explaining that, although some plaintiffs in the suit

had not yet suffered identity theft, allegations that other customers whose data was compromised had reported fraudulent charges helped establish that plaintiffs were at substantial risk of future harm) *with Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343-44 (11th Cir. 2021) (finding standing difficult to meet without "specific evidence of *some* misuse of class members' data").

Rather than clarify the law in this area with its June 2021 decision in the *TransUnion* case, the U.S. Supreme Court chose to follow Salvador Dali's maxim: "What is important is to spread confusion, not eliminate it." Some elements of the Court's reasoning seem to preclude data breach standing based on an elevated risk of future harm. The Court stated that, "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." 141 S. Ct. at 2210-11. The Court also appeared to reject the idea that plaintiffs who have not yet experienced identity theft (Group Three) could tie their standing to those group members who had (Groups One and Two). It emphasized: "[S]tanding is not dispensed in gross; plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *Id.* at 2208. Thus, while concluding that the members of the class whose false credit reports had been disseminated could establish standing, the Court determined that those whose false credit reports had not been sent to third parties (and thus faced only possible future harm) could not proceed as plaintiffs. *Id.* at 2209-13.

However, at least four elements of *TransUnion* have created space for data breach plaintiffs:

- *First*, some courts have distinguished standing challenges at the pleadings stage from *TransUnion*, where there existed the "helpful benefit of a jury verdict." *Id.* at 2222 (Thomas, J., dissenting). Believing that "[s]uch an inquiry may be appropriate after a proceeding on the merits" but not on a motion to dismiss, they have allowed Group Three plaintiffs to "have the benefit of discovery" before definitively addressing standing. *In re: Blackbaud, Inc. Customer Data Breach Litig.*, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021).
- *Second*, other courts have noted that "*TransUnion* involved a suit for statutory damages, not compensatory damages," and have concluded that its holding is inapplicable "to a claim for compensatory damages." *Cotter v. Checkers Drive-In Rest., Inc.*, 2021 WL 3773414, at *4 (M.D. Fla. Aug. 25, 2021).
- *Third*, the *TransUnion* Court specifically noted that "a plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm," but took "no position on whether or how such an emotional or psychological harm could suffice for Article III purposes." 141 S. Ct. at 2211 n.7. Emboldened by this language, at least some courts have since determined that, in the data breach context, "allegations of emotional distress, coupled with the substantial risk of future harm, are sufficiently concrete to establish standing in a claim for damages." *In re: Mednax Servs., Inc. Customer Data Sec. Breach Litig.*, 2022 WL 1468057, at *8 (S.D. Fla. May 10, 2022); *see also Bowen v. Paxton Media Grp., LLC*, 2022 WL 4110319, at *5 (W.D. Ky. Sept. 8, 2022) (same).
- *Fourth*, the Supreme Court in *TransUnion* identified "intrusion upon seclusion" as an "intangible harm" that has been "traditionally recognized as providing a basis for lawsuits in American courts." 141 S. Ct. at 2204. Accordingly, data breach plaintiffs often plead "invasion of privacy" as an example of the "actual and concrete injuries" experienced by Group Three plaintiffs, *see, e.g.*, *Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, Complaint ¶ 13 (C.D. Cal. Sept. 13, 2022), and some courts have concluded that Article III standing exists for this reason alone given that the injury from a data breach is "analogous to that associated with the common-law tort of public disclosure of private information," *Bohnak v. Marsh & McLennan Cos.*, 580 F. Supp. 3d 21, 30 (S.D.N.Y. 2022). *See also Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 43 (D. Ariz. 2021) (similar).

Other courts have rejected these expansive arguments and read *TransUnion* narrowly; they have thus concluded at the pleadings stage that plaintiffs within Group Three lack standing. *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *9-11; *see also Patterson v. Med. Review Inst.*, 2022 WL 3702102, at *2-3 (N.D. Cal. Aug. 26, 2022) (rejecting emotional distress, lost time, and mitigation efforts as groups for standing for Group Three plaintiffs); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 985, 993 (W.D. Okla. 2021) ("Given the holding in *TransUnion*, it is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft following a data breach is still good law, at least with respect to a claim for damages."). Whether a court will credit other related Group Three standing arguments—such as mitigation efforts, loss of value of PI,

lost benefit of the bargain, or overpayment—often depends on whether it reads *TransUnion* in a pro-plaintiff or pro-defendant manner. Those courts that read *TransUnion* in a pro-plaintiff manner tend to find these related standing arguments to be persuasive supplemental grounds for standing, while those courts that view *TransUnion* as a pro-defendant decision reach the opposite result. *Compare In re: Mednax*, 2022 WL 1468057, at *7-9 (crediting such arguments) *with In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *9-11 (rejecting same arguments). Absent further clarification by the U.S. Supreme Court in this area, disparate results based on similar facts are likely to continue. Given the nationwide reach of most data breach litigation, one would expect to see an influx of cases in the coming years in those jurisdictions that have proven thus far to be pro-plaintiff.

Plaintiffs' Approach – A Medley of Creative Claims

a. Federal Law's Minimal Role Thus Far in Private Data Breach Litigation

There have been occasional efforts to pass a federal breach notice law that would preempt state laws and impose a uniform national standard. Advocates have claimed that federalization would produce regulatory simplification and ease the burden faced by companies, who now must comply with scores of different state and territorial laws. For instance, in June 2022, the American Data Privacy and Protection Act ("ADPPA") was introduced by a bipartisan group of House members with the goal of creating a uniform standard of care for data security. Such bills have previously floundered due to concerns that they set the consumer protection bar too low and, through preemption, may intrude on states' longstanding security and consumer protection statutes. Given recent developments, it appears that the ADPPA has met a similar fate.

Absent the enactment of similar legislation, private data breach plaintiffs face a situation where, at least federally, numerous data security laws exist, but none lend themselves particularly well to data breach litigation. To be sure, federal laws such as the Computer Fraud and Abuse Act (CFAA), Driver's Privacy Protection Act (DPAA), the Electronic Communications Privacy Act (ECPA) and its two titles (the Wiretap Act and the Stored Communications Act (SCA)), the Video Privacy Protection Act (VPPA), the Telephone Consumer Protection Act (TCPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are frequently employed by plaintiffs in other cybersecurity contexts, but none are targeted at the precise kinds of claims that data breach plaintiffs wish to make against companies who, because of a breach, have failed to protect their PI. Some data breach plaintiffs have attempted to weaponize the DPPA, which provides for actual damages or liquidated damages in the amount of $2,500 (whichever is greater), punitive damages, reasonable attorneys' fees, and a private right of action. However, courts thus far have been largely unreceptive to DPPA claims in the data breach context. Instead, they have distinguished the DPPA in two ways: (1) it "imposes civil liability only on a defendant who obtains personal information *from* a motor vehicle record, but not on a defendant who merely obtains information that can be linked back to (*i.e.*, derived from) such a record," *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 927 (4th Cir. 2022); and (2) the statute is not triggered because the act of storing driver's license information on unsecured external servers does not constitute "disclosure" within the meaning of DPPA, *Allen v. Vertafore, Inc.*, 28 F.4th 613, 617 (5th Cir. 2022).

Accordingly, due to the limitations of federal law, state statutory and common-law claims have been the primary focus of private data breach litigation to date.

b. The Cornucopia of Options That State Law Provides to Private Litigants

Data breach plaintiffs have pursued scores of disparate state statutory and common-law claims. Such plaintiffs often shoehorn as many as possible into their complaints, thereby adopting a blunderbuss pleading strategy to try to maximize their settlement leverage and preserve as many claims as possible. A court, in addressing these claims, often faces unique problems when undertaking the choice-of-law analysis—especially because the rise of data on the cloud obfuscates the location of the injury (*i.e.*, the breach), which may play an important role in the choice-of-law determination. Further complexity is introduced by the fact that the court may have to juggle separate state contract claims governed by different choice-of-law rules (*e.g.*, the place where the alleged contract was formed, "most significant relationship" test, and "governmental interest" analysis). The court was compelled to address all these issues at the pleadings stage in the *In re: Mednax Servs.* case. *See* 2022 WL 1468057, at *3-5. In short, inventive plaintiffs have a cornucopia of options available to them to make life difficult for defendant-entities, who are already reeling from a breach event.

State Statutory Claims. At present, California is the only state that has adopted a comprehensive consumer privacy statute with a private right of action specifically targeted at redressing data breaches. Virginia (Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 *et seq.*), Colorado (Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 through 6-1-1313), Utah (Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 *et seq.*), and Connecticut (CT SB 6) have also enacted comprehensive consumer privacy statutes in recent years. However, none of these statutes—to date—provides for a

private right of action. The California Consumer Privacy Act (CCPA) went into effect January 1, 2020. Data breach plaintiffs occasionally attempted claims based on the CCPA's predecessor statute, the California Customer Records Act (CRA). *See* Cal. Civ. Code §§ 1798.81-82. It provides a private right of action for unauthorized access, theft, or disclosure of unredacted, unencrypted "personal information" as a result of a business's failure to implement and maintain reasonable security measures and procedures. Cal. Civ. Code § 1798.150(a)(1). The CCPA has since been amended by the California Privacy Rights Act (CPRA). Effective January 1, 2023, the CPRA expands the definition of "personal information" in the CCPA to include biometric data (Cal. Civ. Code § 1798.140(o) (Cal. Civ. Code § 1798.140(v) after Jan. 1, 2023)) and extends the private right of action to consumers whose email addresses, with a password or security question-and-answer that would permit access to that account, are compromised. The CCPA covers all information so long as it relates to a California resident or California household, and applies to all for-profit, private entities that collect PI, do business in California, and meet certain threshold criteria defined in the statute. Cal. Civ. Code § 1798.140(c) (Cal. Civ. Code § 1798.140(d) after Jan. 1, 2023).

The CCPA has driven a significant volume of data privacy litigation since its enactment. Despite the relatively narrow scope of the statute, there were over 125 cases filed within a year of its effective date that asserted CCPA claims, and there have been at least 17 settlements in class actions in which a CCPA claim was asserted. CCPA cases have already survived pleadings-stage challenges. *See, e.g.*, *Karter v. Epiq Sys., Inc.*, 2021 WL 4353274, at *2-3 (C.D. Cal. July 16, 2021). The statute's popularity among data breach plaintiffs can be traced to the damages it provides for private actions, which include: (1) the greater of a statutory amount between $100 and $750 per consumer per incident and actual damages; (2) declaratory or injunctive relief; and (3) any other relief the court deems proper. Cal. Civ. Code § 1798.150(a). While certain aspects of the CCPA have yet to be fully resolved, including the "notice and cure" provision available to defendants, Cal. Civ. Code § 1798.150(b), the presence of CCPA claims has made California subclasses a common occurrence in data breach class actions. Members of these California subclasses are typically offered additional monetary compensation—often $50 to $100 more than the settlement benefits offered to the nationwide class—to account for the availability of statutory penalties under the CCPA.

State Common-Law Claims. Private data breach plaintiffs also have a wide array of state common-law claims at their disposal, many of which have proven effective. Typically asserted claims include: (1) negligence; (2) gross negligence; (3) negligence per se; (4) breach of express contract; (5) breach of implied contract; (6) breach of the implied duty of good faith and fair dealing; (7) breach of fiduciary duty/confidence; (8) unjust enrichment; and (9) invasion of privacy or intrusion upon seclusion *See, e.g.*, *Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶¶ 113-94 (C.D. Cal. Sept. 13, 2022); *In re: Rutter's Inc.*, 511 F. Supp. 3d at 520; *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1365 (N.D. Ga. 2021). While the success of these claims often depends on the specific facts alleged and the precise contours of the law in the applicable jurisdictions, certain obvious trends have emerged.

Negligence claims. Data breach plaintiffs typically allege that, given previous data breach incidents (including in the same industry), the defendant was on notice that a foreseeable risk of a data breach existed. *See Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶¶ 45-50 (C.D. Cal. Sept. 13, 2022). They further contend that the defendant failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines and frameworks such as the NIST Cybersecurity Framework, the Federal Risk and Authorization Management Program, and/or the Center for Internet Security's Critical Security Controls. *See id.* ¶¶ 65-70; Krefting *v. OneTouchPoint, Inc.*, No. 2:22-cv-01052, ECF Doc. # 1, compl. ¶ 60 (E.D. Wisc. Sept. 12, 2022). Most states recognize a common-law duty to take "reasonable precautions" to prevent injury by a third party (*i.e.*, the hacker) where the defendant created a situation it knew or should have known posed a substantial risk to a plaintiff (*i.e.*, its intentional collection and storage of plaintiffs' PI). As such, courts frequently conclude that data breach plaintiffs have adequately alleged claims for negligence and gross negligence. *See, e.g.*, *In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *14-15; *In re: Blackbaud, Inc. Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 679-83 (D.S.C. 2021); *Purvis*, 563 F. Supp. 3d at 1366-71; *In re: Rutter's Inc.*, 511 F. Supp. 3d at 526-30.

Contract claims. Many companies that obtain or handle PI provide users or customers with a privacy notice that contains certain representations concerning their compliance with federal law and their protection of PI from unauthorized access and use. In addition, it is common for companies to include statements on their websites and in other materials as to the importance they place on data security, their use of strong encryption to protect PI, and their prohibition of unlawful disclosure of that PI. Data breach plaintiffs often cite these notices, policies, and statements as establishing an express or implied contract that the defendant then breached

through its lax security measures. Defendants usually respond by contending that such statements are not enforceable promises (only broad depictions of corporate policy), there was no enforceable agreement due to a lack of mutual assent/meeting-of-the-minds, and plaintiffs failed to allege that they read or were even aware of any terms of the privacy notice. *See In re: Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 410 (E.D.Va. 2020) (outlining defenses). While some courts have found these defenses to be persuasive at the pleadings stage, data breach plaintiffs have experienced a surprising amount of success with express and implied breach of contract claims, *see, e.g.*, *In re: Rutter's*, 511 F. Supp. 3d at 533-37 (collecting cases); *Purvis*, 563 F. Supp. 3d at 1379-82; *In re: Capital One*, 488 F. Supp. 3d at 410-11. Claims for breach of the implied covenant of good faith and fair dealing are more likely to fail, as such claims are often duplicative of or subsumed by contract claims under state law. *See In re: Mednax Servs.*, 2022 WL 1468057, at *13-14 (dismissing implied covenant claim for this reason).

Breach of duty claims. Data breach plaintiffs often have a difficult time pleading plausible claims for breach of fiduciary duty. Courts are generally loath to find that the receipt of PI by a business transforms an arm's-length transaction into a fiduciary relationship. *See id.* at *27-28. The same is generally true when companies gather PI in connection with employment, which many courts view as a common practice that does not typically suggest that the employee is trusting their employer in "unique or exceptional ways." *Purvis*, 563 F. Supp. 3d at 1384. Breach of fiduciary duty claims tend to be more successful where PHI has been breached and the defendant is a healthcare provider, as some states recognize that the provision of medical care suggests a confidential relationship. *Id.* at 1383. Claims for breach of confidence are similarly difficult to maintain, as typically there are no facts to suggest that the defendant *disclosed* the PI or PHI to a third party. Absent this required element, the defendant's inadequate security may support a claim in negligence but not breach of confidence. *Id.* at 1378.

Unjust enrichment claims. "[F]ederal courts are not uniform in their analyses of unjust enrichment claims in data breach class actions." *In re: Rutter's Inc.*, 511 F. Supp. 3d at 538. The outcome often "depends on the level of deference a court affords a plaintiff's allegations" at the pleadings stage, what the defendant does with the PI, and the type of business in which the defendant is involved. *Id.* As a general rule, where the defendant is a business that commoditizes the PI or receives an independent pecuniary benefit from holding the PI (such as using it to better target customers and increase profits), the more likely it is that a court will allow the private data breach plaintiffs' unjust enrichment claim to proceed. *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *18. The same is true if the very nature of the defendant's business involves obtaining and protecting PI (such as where the defendant is a credit card company). *See In re: Capital One*, 488 F. Supp. 3d at 411-13. Unjust enrichment claims have been less successful outside of these contexts and are especially fraught where the defendant does not directly profit from the PI (such as where the defendant is a medical provider). *See In re: Blackbaud*, 567 F. Supp. 3d at 687-88; *In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *18

Privacy claims. Stand-alone tort claims for invasion of privacy or intrusion into private affairs/seclusion have generally fared poorly in private data breach litigation. In many jurisdictions, such claims are "intentional" torts for which mere negligence will not suffice. But data breach plaintiffs can rarely allege that defendants intentionally disclosed their PI or PHI to unauthorized persons. Rather, a third party (the hacker) typically carries out the data breach without the active participation of the defendant corporation. Because "negligence does not morph into an intentional act of divulging [plaintiffs'] confidential information," such claims are often subject to dismissal. *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1288 (N.D. Ala. 2014); *see also In re: Mednax Servs.*, 2022 WL 1468057, at *26-27 (collecting cases); *Purvis*, 563 F. Supp. 3d at 1377-78.

What's Next?

Defendants should expect to see novel injury theories with increasing frequency as data breach law continues to mature. Litigation exposure will be difficult to gauge in the near term, especially given the dearth of clear precedent and material differences in both the standing and merits analyses undertaken by different jurisdictions. Litigation risk will also increase as data breaches become more prevalent and affect greater numbers, as even nominal damages—when aggregated—can produce extraordinary recoveries. And, although most data breach cases are brought on behalf of plaintiffs whose PI was actually or potentially accessed, spillover into other areas is likely. For instance, shareholders may increasingly seek to hold executives and board members liable for failing to adopt "reasonable security measures" to prevent cybercrime.

But not all innovation will occur on the plaintiffs' side. As data breach plaintiffs become ever more imaginative, we anticipate that defendants will take steps often seen in other class action contexts to blunt their leverage. Through clickwrap or similar agreements, more companies may shift to a model in which their consumers, users, employees, or patients consent to a "privacy policy" in which they (1) agree to take administrative steps, such as providing written notice or engaging in an informal

dispute resolution, before their breach-related claims are ripe; (2) agree to arbitrate their claims; (3) waive their ability to seek relief on a class-wide or representative basis; and/or (4) agree to waive their non-statutory claims in return for the defendant's services. Indeed, at least some courts seem receptive to these ideas in the data breach context. Undoubtedly, defendants also will continue to make attacks on the fundamental ability of data breach plaintiffs to certify a viable class where individual issues often predominate.

But given this uncertain milieu, it is critical that companies engage with experienced counsel to ensure compliance with prescriptive requirements, design and execute a breach response plan, and develop the optimal data breach litigation strategy.

NOTED WITH INTEREST

Update on Section 101 Patent Eligibility Law: *American Axle* and the Patent Eligibility Restoration Act

On June 30, 2022, the Supreme Court denied cert in *American Axle v. Neapco,* a Federal Circuit decision regarding patent eligibility. The patent community had been looking to this case as way to bring much-needed clarity to Section 101 caselaw following the Supreme Court's 2012 and 2014 decisions in *Alice/Mayo*, but unfortunately the Supreme Court's denial refuses to provide that clarity. A new bill introduced by Senator Thom Tillis aims to provide new guidance as well, but has been criticized for its inclusion of ambiguous language that could lead to even more patent-eligibility litigation.

Background on Section 101: Section 101 of the U.S. Patent Act provides that whoever "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." Over the years, the Supreme Court has found several exceptions to subject-matter eligibility that are not based in the statute. For example, natural laws, natural phenomena, and abstract ideas are not eligible to be patented. *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980). Almost every invention, however, relies on natural phenomena. And almost every invention can be described in abstract terms. So where does the line get drawn?

The Supreme Court attempted to clarify this distinction in two cases, *Mayo v. Prometheus*, 566 U.S. 66 (2012), and *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014). The resulting test, commonly referred to as the *Alice/Mayo* test, consists of two steps. First, courts consider whether the claims at issue are directed to an ineligible concept (*i.e.*, abstract ideas or natural laws). This is done by comparing the claimed concept to other inventions that were previously found to be ineligible. If the concepts are sufficiently similar, courts then need to decide whether each claim, or all the claims taken together, provide "something more" that transforms the nature of the claim into a patent-eligible application.

Already, the fuzzy nature of this test is apparent. What constitutes "sufficiently similar"? Or "something more?" After the *Alice* decision, a slew of subject matter ineligibility rulings were decided on nearly identical grounds in the lower courts: the claim(s) were invalid because they were directed to an abstract or natural concept and didn't provide anything "more." After finding that application of the *Alice/Mayo* test "in a consistent manner has proven to be difficult," the USPTO issued new guidance that aimed to provide more clarity and certainty to both patent infringers and owners. *See* 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019). In particular, the USPTO broke the first step of the *Alice/Mayo* test into two subparts: (1) "[p]roviding groupings of subject matter that [are] considered an abstract idea"; and (2) "clarifying that a claim is not 'directed to' a judicial exception if the judicial exception is integrated into a practical application of that exception."

And yet, just a few months later, the Federal Circuit rejected the USPTO's guidance by affirming the then-current application of the *Alice/Mayo* test in *American Axle*. The Federal Circuit has also since confirmed that the USPTO's guidance "does not carry the force of law, and is not binding on [its] patent eligibility analysis." *cxLoyalty, Inc. v. Maritz Holdings Inc.*, 986 F.3d 1367, 1376 (Fed. Cir. 2021).

***American Axle*:** The case started in 2015 when American Axle, a manufacturer of automobile components, sued its competitor, Neapco, for patent infringement. The patent claim in question involved methods of reducing vibration on the propeller shaft assembly of a vehicle. The district court found that the patent was ineligible under Section 101 because the asserted claims merely suggested the application of Hooke's law, a well-known equation that describes the relationship between an object's mass, its stiffness, and the frequency at which the object vibrates, and otherwise didn't add anything

beyond "well-understood, routine, conventional activity already engaged in by the scientific community." *Am. Axle & Mfg., Inc. v. Neapco Holdings LLC*, 309 F. Supp. 3d 218 (D. Del. 2018).

In July 2020 the Federal Circuit affirmed the district court's holding, finding that the asserted claims "simply require[] the application of Hooke's law to tune a propshaft liner to dampen certain vibrations." *Am. Axle & Mfg, Inc. v. Neapco Holdings LLC*, 967 F.3d 1285, 1292 (Fed. Cir. 2020). Judge Moore strongly dissented, arguing that the claims at issue offer a "specific, concrete solution (inserting a liner inside a propshaft) to a problem (vibrations in propshafts)," and the majority's refusal to recognize them as patentable under Section 101 is "likely to create confusion for the district courts and to expand § 101 profoundly." *Id.* at 1304-05.

After a denial of rehearing *en banc*, four separate dissenting opinions emerged. Judge Newman, one of the chief dissenters, noted that "[t]he court's rulings on patent eligibility have become so diverse and unpredictable as to have a serious effect on the innovation incentive in all fields of technology." On appeal to the Supreme Court, the Solicitor General and various prominent amici (including IP bar associations, a member of Congress, and even a former Chief Judge of the Federal Circuit and former director of the USPTO) argued that the Supreme Court should take this case up to clarify the law in this area. The Supreme Court nevertheless denied cert, leading to some disappointment in the patent community.

Patent Eligibility Restoration Act: There have also been efforts within Congress to set more precise rules for the patent eligibility test. On August 2, 2022, Senator Thom Tillis (R-NC) introduced the Patent Eligibility Restoration Act, specifically citing the Supreme Court's refusal to weigh in on *American Axle* as a motivating factor for the bill. The text of the bill retains much of the original wording of Section 101 but attempts to specifically define concepts that are not patent-eligible such as mathematical formulas, processes performed solely in the human mind, unmodified natural materials, and processes that occur in nature independent of human activity. The bill also clarifies that "non-technological economic, financial, business, social, cultural, or artistic process[es]" are not patent eligible.

Overall, the bill aims to expand the scope of what courts find to be patent eligible. *First*, it provides that abstract ideas or laws of nature are only ineligible if they are claimed "as such." This language is apparently designed to address the trend of courts finding that a patent is ineligible because it is "directed to" an abstract idea. Under Senator Tillis' proposed bill, such a patent would only be ineligible if it specifically claims an abstract idea—a narrower formulation, but one which some view as ambiguous. *Second,* the bill provides that patent eligibility should be determined by considering the claimed invention as a whole, rather than on a claim-by-claim basis. This means that a claim with a combination of eligible and ineligible subject matter could still be found eligible, whereas under *Alice/Mayo* such claims would often be found ineligible. *Third*, the bill provides that whether a claim is novel or nonobvious should have no place in the eligibility analysis, as these considerations are governed by other parts of the law.

* * * *

Some feel that the continued lack of clarity around patent eligibility under Section 101 has made it difficult for inventors, businesses, patent examiners, and trial judges to reliably determine what subject matter is patent-eligible. These questions may remain unanswered until the Supreme Court decides to take up its next patent eligibility case, and many see *American Axle* as a missed opportunity. Whether the Patent Eligibility Restoration Act provides any clarity to Section 101 caselaw also remains to be seen. Introducing a bill is a first step in a long process of revisions that could take years (and still never pass). And even if it does pass, whether the bill provides the requested clarity is yet another question.

PRACTICE AREA NOTES

Securities & Structured Finance Litigation Update

The Decline of State Court Securities Act Claims: 2022 Trends Post-*Cyan*

In 2018, the Supreme Court issued its decision in *Cyan v. Beaver County Employees Retirement Fund*, 138 S. Ct. 1061 (2018), which held that claims under the Securities Act of 1933 (the "Securities Act") could proceed in state court and thereby evade certain defendant-friendly restrictions that are otherwise mandated in federal court. Since that time, securities issuers have attempted to get around the Court's decision in *Cyan*, utilizing various strategies both to prevent the filing of state court claims under the Securities Act and to ensure that state courts provide the same protections that are available in federal court. This article explores the treatment of those actions when challenged in state court and anticipated trends in state court securities litigation going forward.

The Securities Act of 1933 and the Supreme Court's Decision in *Cyan*

The Securities Act provides certain private rights of action for materially false or misleading statements contained in securities registration statements, which claims may be brought in either federal or state court. 15 U.S.C. § 77k. In 1995, recognizing and seeking to curb abuses of the federal securities laws, Congress enacted the Private Securities Litigation Reform Act (the "PSLRA"). Among other things, the PSLRA mandates sanctions for frivolous litigation, imposes a heightened pleading standard for certain claims, creates a "safe harbor" for forward looking statements and prohibits discovery until after a complaint has survived a motion to dismiss. 15 U.S.C. § 77z-1.

Following the enactment of the PSLRA, securities plaintiffs flocked to state court with their securities claims, seeking to avoid the strictures of that legislation. Congress addressed this trend in 1998 with the passage of the Securities Litigation Uniform Standards Act ("SLUSA"), which made federal court the exclusive forum for all fraud-based securities class actions. In doing so, however, Congress left open the ability of plaintiffs to file certain Securities Act claims (among them, Sections 11, 12 and 15) in state court, as those claims require a plaintiff to prove only a misrepresentation, not fraud. And although the defense bar subsequently attempted to extend the benefits of the PSLRA to these claims, those attempts were addressed—and rejected—by the Supreme Court in *Cyan*, which acknowledged that if Securities Act claims proceed in state court, plaintiffs can evade some of the PSLRA's requirements, contrary to the policy rationale underlying SLUSA, but held regardless that SLUSA neither deprived state courts of jurisdiction over these actions nor granted defendants the right to remove.

Federal Forum Selection Clauses

A predictable influx of state court Securities Act litigation followed in the wake of the Supreme Court's ruling in *Cyan*. In response, issuers of securities began amending their articles of incorporation to require that Securities Act claims be brought only in federal court. Plaintiffs, in turn, challenged the legality of these decisions. In 2020, the Delaware Supreme Court—reversing the Chancery Court —, held that such provisions re valid under the Delaware statutes governing certificates of incorporation, and that they violated neither Delaware nor federal law or policy." *Salzberg v. Sciabacucchi*, 227 A.3d 102 (Del. 2020). The court recognized, however, a question "down the road" as to whether federal forum selection provisions would "be respected and enforced" by other states, observing that the "question of enforceability is a separate, subsequent analysis that should not drive the initial facial validity inquiry." *Id.*

Wong v. Restoration Robotics, Inc., 78 Cal. App. 5th 48 (1st Dist. 2022), issued on April 28, 2022 by the California Court of Appeals, provides the first authoritative answer to this question in a California appellate court. In particular, the Court of Appeal in *Wong* agreed with the Delaware Supreme Court in finding that federal forum selection provisions are valid and enforceable, that they do not violate the Securities Act, and that they do not represent an "unconscionable" act by a party with superior bargaining power. The Court of Appeal reached the same result 15 days later in *Simonton v. Dropbox, Inc.*¸No. A161603 (Cal. Ct. App. May 13, 2022), a case in which the firm was involved. Although not binding on other states, the decisions by the California Court of Appeal, in what some view as a pro-plaintiff jurisdiction, may signal that federal forum provisions will be enforced by state courts around the country, ultimately leading to a significant decrease in state court Securities Act claims.

Applicability of PSLRA Discovery Stay to Securities Act Litigation in State Court

One of the main benefits of the PSLRA to defendants is that it imposes an automatic stay of discovery during the pendency of a motion to dismiss, in "any private action arising under" the Securities Act. § 77z-1(b). This prevents plaintiffs from coercing defendants into early settlement of unmeritorious claims rather than bearing steep discovery costs. While the stay applies undisputedly to claims brought in federal courts, state courts across the country have reached conflicting conclusions on this issue. *See In re Greensky, Inc. Sec. Litig.*, 2019 WL 6310525, at *1 (N.Y. Sup. Ct. Nov. 25, 2019) ("Courts, even in this County, are split on whether the stay set forth in the Private Securities Litigation Reform Act of 1995 (the PSLRA) necessarily applies to state proceedings.").

Several courts have concluded that the stay applies in both federal and state court. *See, e.g., id.*; *City of Livonia Retiree Health and Disability Benefits Plan v. Pitney Bowes inc.*, 2019 WL 2293924, at *4 (Conn. Super. May 15, 2019); *In re Everquote, Inc. Sec. Litig.*, 106 N.Y.S.3d 828, 828 (N.Y. Sup. Ct. 2019). A majority of state courts, however, have refused to apply the discovery stay to state court actions—including California, generally considered a plaintiff-friendly jurisdiction whose state courts have primarily rejected attempts by litigants to apply the PSLRA's discovery stay. *See, e.g., In re Pivotal Software, Inc. Securities Litigation*, Case No CG19576750 (San Fran. Super. Ct. Mar. 4, 2021); *Switzer v. Hambrecht & Co., L.L.C.*, 2018 WL 4704776, at *1 (San Fran. Super. Ct. Sept. 18, 2018); *Plymouth Cnty. Contributory v. Adams Pharms., Inc.*, No. RG19018715 (Alameda Super. Ct. July 26, 2019); *see also In re Dentsply Sirona, Inc.*, 2019 WL 3526142, at *6 (N.Y. Sup. Ct. Aug. 2, 2019); *In re*

PPDAI Group Sec. Litig, 116 N.Y.S.3d 865, at *6-7 (N.Y. Sup. Ct. 2019).

However, on July 25, 2022, as what appears part of a growing trend, a California state court held that the PSLRA's automatic discovery stay *does apply* to claims filed in state court under the Securities Act. *See Ocampo v. Williams*, 21-CIV-03843 (San Mateo Super. Ct. July 25, 2022). In doing so, the court in *Ocampo* recognized that giving the phrase "***any*** private action arising under this subchapter" its "ordinary meaning" meant that the stay should apply in state court actions. The court then considered statutory context, ultimately determining that the Supreme Court has held that similarly worded provisions (*i.e.*, the safe harbor) operate in both state and federal court, and thus the discovery stay should as well. Finally, the *Ocampo* court urged the US Supreme Court to provide the "last word" on this issue "as soon as possible." The import of this decision is clear: ultimately, if state courts continue to follow suit, or if the Supreme Court takes up the issue and agrees, securities plaintiffs would possess less settlement leverage in state court actions.

Notably, the Supreme Court has previously attempted to resolve this issue, granting certiorari to review a decision by the California Superior Court denying a request to apply the stay in *Pivotal Software, Inc. v. Superior Court*, 141 S. Ct. 2884 (2021). However, prior to completion of merits briefing, the case settled, leaving the issue open and ripe for consideration in another case. Given this, it is plausible that the Supreme Court may be willing to grant review again should the opportunity arise.

Anticipated 2023 Trends

Following the Supreme Court's decision in *Cyan*, in 2019 there were 52 state court Securities Act claims filed. *See* Cornerstone Research: Securities Class Action Filings, https://securities.stanford.edu/research-reports/1996-2022/Securities-Class-Action-Filings-2022-Midyear-Assessment.pdf, at 15, Figure 14 ("Cornerstone Report"). However, from 2019 to 2021, the year following the Delaware Supreme Court's decision in *Sciabacucchi*, the number of Securities Act claims filed in state court dropped 77% to 12. *Id.* at 4. "If H1 trends continue, state [Securities Act] filings [in 2022] will be only around 23% of their 2019 levels." *Id.* "Only 27% of total [Securities Act] filings were brought in state court in [the first half of 2022], with or without a parallel filing. This is the lowest level since [the second half of 2014] and continues the decline since its peak at 86% in [the second half of 2018]." *Id.* at 17. Notably, three of the six state Securities Act claims filed in the first half of 2022 were in California, and were filed prior to the *Restoration Robotics* and *Ocampo* decisions. *Id.* at 15, Figure 14. Given the recent receptiveness of courts—California courts in particular—to issuers' attempts to limit their exposure to state court securities actions and to extend the protections afforded in federal court under the PSLRA, it is likely that these trends will continue, with the number of actions filed in state court continuing to decline.

Life Science Update

The issue of what is or is not patent-eligible subject matter under 35 U.S.C. § 101 has been hotly contested over the past decade. The debate stems largely from two U.S. Supreme Court decisions on the topic, as well as a large body of caselaw from the U.S. Court of Appeals for the Federal Circuit, which has been criticized for lacking uniformity. The Federal Circuit's recent § 101 decision in *American Axle & Manufacturing, Inc., v. Neapco Holdings LLC*, 967 F.3d 1285 (Fed. Cir. 2020), has further intensified that debate both as a general matter and specifically within the life sciences industry.

I. *American Axle*

American Axle involved a patent claiming a method of manufacturing an automobile drive shaft that involved the use of a liner that was "tuned" to reduce the drive shaft's vibration, making it quieter. 967 F.3d at 1289. Prior to *American Axle*, such patent claims fell within the category of claims that have traditionally been considered patent-eligible under § 101. A divided Federal Circuit panel held, however, that the claims were directed to patent ineligible subject matter. Id. at 1288. Specifically, the panel majority found that, even though neither the claims nor the specification explicitly referenced a natural law, the method required the use of a natural law—Hooke's law, which describes the relationship between an object's mass, its stiffness, and the frequency at which it vibrates—"and nothing more." *Id.* at 1297. According to the majority, the claims recited only a desired result without "limiting the claim to particular methods of achieving the result. . . ." *Id.* at 1295. According to the panel, to be patent-eligible, a claim "must go beyond stating a functional result; it must identify 'how' that functional result is achieved by limiting the claim scope . . . to concrete action, in the case of a method claim." *Id.* at 1302.

Although the majority in *American Axle* stressed that its decision was consistent with Supreme Court and Federal Circuit precedent on § 101, *see* 967 F.3d at 1296 ("[o]ur cases as well have consistently rejected such claims as unpatentable."), others saw it as a broad expansion of the doctrine. Indeed, Judge Kimberly Moore dissented, arguing that the majority conflated the § 101 requirement with that of enablement under § 112 and thus expanded § 101 beyond its intended gatekeeping role. *Id.* at 1305 (Moore, J., dissenting).

The Federal Circuit denied rehearing en banc and *American Axle* filed a petition for certiorari. Several Judges dissenting from the denial of en banc rehearing echoed Judge Moore's concerns and called for the Supreme Court to grant certiorari and provide clarification to the lower courts. *See, e.g.*, *Am. Axle & Mfg., Inc. v. Neapco Holdings LLC*, 966 F.3d 1347, 1357 (Fed. Cir. 2020) (Newman, J., dissenting) ("The court's rulings on patent eligibility have become so diverse and unpredictable as to have a serious effect on the innovation incentive in all fields of technology.").

So too did the Solicitor General in its response to the Supreme Court's request for its view on the matter. *See* Brief for the United States as Amicus Curiae at 19, 21, *Am. Axle & Mfg., Inc. v. Neapco Holdings LLC*, 142 S. Ct. 2902, 2022 WL 1670811 (2022) (noting that "[t]his is only the most recent Section 101 case that has fractured the Federal Circuit," and that "[t]his case is a suitable vehicle for providing greater clarity").

Nonetheless, the Supreme Court denied *American Axle*'s petition in June of last year.

To many, the Supreme Court's denial was unsurprising. From this perspective *American Axle* was just one of a long list of § 101 cases that the Court has declined to hear since its decisions in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S. Ct. 1289 (2012), and *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014). Given the Supreme Court's most recent reminder of its apparent reluctance to take up § 101 cases, there has been a renewed interest in legislative reform.

II. Proposed Legislation

Senator Thom Tillis (R-NC) proposed a new bill this past August called the Patent Eligibility Restoration Act of 2022. According to a Press Release issued by Senator Tillis' office, "current Supreme Court[] patent eligibility jurisprudence is undermining American innovation and allowing foreign adversaries like China to overtake us in key technology innovations." *See* Press Release, Tillis Introduces Landmark Legislation to Restore American Innovation (Aug. 3, 2022). The Press Release describes the bill as addressing those concerns by "by enumerating a specific but extensive list of excluded subject matter." *Id.* Specifically, the bill keeps the current language of § 101—"[w]hoever invents or discovers any useful process, machine, manufacture, or composition of matter, or any useful improvement thereof, may obtain a patent therefore"—but adds a subsection (B) which provides statutory exceptions on subject matter for which "a person may not obtain a patent." Those exception are: "(A) A mathematical formula, apart from a useful invention or discovery"; "(B) [a] process that—(i) is non-technological economic, financial, business, social, cultural, or artistic process; (ii) is a mental process performed solely in the human mind; or (iii) occurs in nature wholly independent of, and prior to, any human activity"; "(C) [a]n unmodified gene, as that gene exists in the human body"; and " (D) [a]n unmodified natural material, as that material exists in nature."

The bill goes on to state that "[f]or purposes of subparagraphs (C) and (D) . . . a human gene or natural material that is isolated, purified, enriched, or otherwise altered by human activity, or that is otherwise employed in a useful invention or discovery, shall not be considered to be unmodified." It also proposes a revision to the definition of the term "process," laid out in 35 U.S.C. § 100, which would replace "includes a new use of a known process" with "includes a use, application, or method of manufacture of a known or naturally-occurring process."

Prior to Senator Tillis' introduction of the Patent Eligibility Restoration Act of 2022, several Senators, including Tillis, requested a report from the USPTO detailing "the current state of patent eligibility jurisprudence in the United States." *See* Letter to USPTO (Mar. 5, 2021), available at https://www.tillis.senate.gov/services/files/04D9DCF2-B699-41AC-BE62-9DCA9460EDDA. The Senators stated that they were "particularly interested in learning how the current jurisprudence has adversely impacted investment and innovation in critical technologies like . . . precision medicine, diagnostic methods, and pharmaceutical treatments," among others. *Id.*

The USPTO submitted its response to that request this June: a report titled "Patent eligible subject matter: Public views on the current jurisprudence in the United States," which based its findings on 141 public comments from a variety of stakeholders including legal associations, industry organizations, advocacy groups, nonprofit entities, businesses, law firms, practitioners, academics, and inventors. At a high level, the Report found that "[t]hose critical of the current state of the law included many patent practitioners and innovative companies, especially companies involved in life sciences" who noted that "making patents less available and rights less predictable, inhibits investment in new technologies and companies." Patent eligible subject matter: Public views on the current jurisprudence in the United States at 3 (June 2022).

In large part, the view of the commentators from the life sciences industry largely echoed Judge Newman's statements in her dissent to the Federal Circuit's decision not to rehear *American Axle* en banc.

As detailed in the report, several life sciences industry participants noted that, because "the development of biologics and pharmaceuticals is both high risk and high cost," "the uncertainty in the current jurisprudence is significantly diminishing present investment in these areas

and disincentivizing future investment and innovation because of the increasingly uncertain prospects of obtaining and enforcing patent rights on these technologies." *Id.* at 26. This, according to an organization representing the biotechnology industry, jeopardizes the life sciences industry's ability to develop and deliver precision medicine, pharmaceutical treatments, and diagnostics to patients." *Id.* at 25. That organization also raised concerns that the current jurisprudence is stifling competition by making it harder for startups and other small and medium-sized entities to attract investments. *Id.* at 27. Another commentator noted that the uncertainty engendered by the current state of law will "force companies seeking to advance this field to protect their intellectual property through trade secrets," which will ultimately slow the progress of science. *Id.* at 32-33.

In late September, Senator Chris Coons (D-DE) announced that he would co-sponsor the bill. Even with a co-sponsor, it is unclear whether the Patent Eligibility Restoration Act of 2022 will pass. Senator Coons and Tillis have noted, however, that they are optimistic about the prospects for intellectual property legislation in the next congress.

III. Conclusion

To many, the Federal Circuit's decision in *American Axle* raised more questions than it answered. What claims are "directed to" a natural law and which are not if the claims need not explicitly recite a natural law to be "directed to" one? What constitutes a "concrete action" as opposed to an unpatentable "functional result"? Under *American Axle*, these questions could certainly be relevant to patent claims in the life sciences field, which can be directed to drug compounds, pharmaceutical formulations, methods of treatment, methods of making drug compounds, and methods of diagnosis, just to name a few. Depending on the creativity of a patent challenger, all of these types of claims could—in theory at least—be framed as depending on the "results" of "natural laws." Thus, the full effect of *American Axle*, particularly to life sciences patents, remains to be seen. In the near term, the only thing that seems certain is that courts, Congress, patent practitioners, and industry leaders will continue to grapple with the scope and applicability of § 101's patent eligibility requirement.

Product Liability Litigation Update

On July 4, 2022, Judge David A. Faber of the United States District Court for the Southern District of West Virginia entered a bench trial verdict in favor of defendants AmerisourceBergen Drug Corporation, Cardinal Health, Inc., and McKesson Corporation, three wholesale distributors of opioids. The plaintiffs in the case are the city of Huntington and Cabell County, both in West Virginia. The plaintiffs asserted only one claim, public nuisance, against the distributors. As a remedy, the plaintiffs proposed an equitable "abatement plan," which would have provided $2.5 billion to the West Virginia city and county. The Court ruled that (1) West Virginia law does not recognize public nuisance claims based on the sale and distribution of products, (2) even if West Virginia did recognize such a claim, the plaintiffs failed to prove the elements of that claim, (3) the alleged misconduct of the distributors did not proximately cause the damages suffered by the plaintiffs, and (4) the plaintiffs' abatement plan was not a proper remedy.

The court ruled that the sale and distribution of products cannot constitute a public nuisance under West Virginia law. The Supreme Court of Appeals of West Virginia has not yet ruled on this issue, so the federal district court made a prediction of what the West Virginia high court would decide under *Erie R.R. Co. v. Tompkins*. In predicting that the West Virginia Supreme Court of Appeals would not extend public nuisance law to the sale and distribution of products, the district court relied on the Restatement (Third) of Torts. (The West Virginia high court has followed the Restatement (Second) of Torts in crafting their nuisance law in the past.) The district court's holding is inconsistent with two lower court decisions in West Virginia state court. *See Brooke Cnty Comm'n v. Purdue Pharma L.P.*, No. 17-C-248, 2018 WL 11242293, at *7 (Marshall Cnty. Cir. Ct. Dec. 28, 2018); *State ex rel. Morrisey v. AmerisourceBergen Drug Corp.*, No. 12-C-141, 2014 WL 12814021, at *8-*10 (Boone Cnty. Cir. Ct. Dec. 12, 2014). The district court found the Oklahoma Supreme Court's reasoning more persuasive. In *State ex rel. Hunter v. Johnson & Johnson*, 499 P.3d 719, 721 (Okla. 2021), the Supreme Court of Oklahoma declined to extend Oklahoma public nuisance law to the manufacturing, marketing, and selling of opioids. The district court noted that "[t]o apply the law of public nuisance to the sale, marketing and distribution of products would invite litigation against any product with a known risk of harm, regardless of the benefits conferred on the public from proper use of the product."

The court also ruled that, even if a public nuisance claim were available, the City and County failed to prove the elements of that claim. A public nuisance is defined as "an unreasonable interference with a right common to the general public." *Duff v. Morgantown Energy Assocs.*, 421 S.E.2d 253, 257 n.6 (W.Va. 1992). The court found that the plaintiffs did not show that the distributors' conduct interfered with a public right. In making this finding, the court balanced the dangers of opioids against the public benefits of responsible opioid use. The court ultimately found that the distributors shipped prescription opioid pills to licensed pharmacists so patients could access the

medication they were prescribed by doctors who were acting in good faith. The court found this conduct to be reasonable.

The court found that the distributors' conduct did not proximately cause the damages suffered by the City and County. In West Virginia, wrongful conduct is a proximate cause only if it "is the last negligent act contributing to the injury." *Sergent v. City of Charleston*, 549 S.E.2d 311, 320 (W. Va. 2001). The court found no proximate cause because (1) it was doctors—not distributors—who determined the volume of opioids dispensed in the City and County, and (2) the diversion of opioids from their legitimate use was due to the intervening criminal acts of third parties.

Finally, the court ruled that the plaintiffs' "abatement plan" was not a proper remedy. Abatement is an equitable remedy. Traditionally, it has taken the form of an order enjoining the defendant from continuing the nuisance-causing conduct. The court noted that although the City and County called their remedy an "abatement plan," the plaintiffs were really seeking "remuneration for the cost of treating the horrendous downstream harms of opioid use and abuse." The $2.5 billion dollars sought by the plaintiffs was not accompanied by a request for an order that the defendants stop distributing opioids (the conduct alleged to be wrongful).

Judge Faber ruled that the City of Huntington and Cabell County's claims against three opioid distributors failed because West Virginia law did not recognize such a claim, the elements of that claim (including causation) had not been met, and the remedy sought was improper. The impact of this case is yet to be seen. On the one hand, the ruling is confined to the law of West Virginia and only addresses public nuisance claims. Moreover, the City and County could appeal the case to the United States Court of Appeals for the Fourth Circuit, which could either disagree with the district court's legal conclusions or ask the West Virginia Supreme Court of Appeals to weigh in. *See* W. Va. R. App. P. 17 (allowing certified questions). On the other hand, the court referenced general principles of nuisance law and remedies, and its holding was independently supported by findings of fact, which are reviewed on appeal only for clear error and which other courts may find persuasive.

VICTORIES

$1 Billion Cash Settlement in Delaware Securities Case

In November 2022, a Quinn Emanuel team secured a **$1 billion cash settlement** (which currently remains subject to judicial approval) on behalf of a class of former Class V common stockholders of Dell Technologies, in a breach-of-fiduciary-duty action against Dell's controlling stockholders Michael Dell and Silver Lake Partners, members of Dell's board of directors, and Dell's financial advisor Goldman Sachs.

The case concerns Dell's 2018 redemption of its Class V common stock in a transaction that paid minority stockholders billions of dollars less than the fair value of their Class V shares. Class V stock was a "tracking stock," a unique security designed to track, on a one-to-one basis, the public trading price of another company's stock, VMware. Dell issued Class V stock to pay for its acquisition of VMware; because Dell could give VMware's former owners only so much cash, Dell financed most of the acquisition with Class V tracking stock. But despite Class V's purported design, it traded at a steep and persistent 30-40% discount to VMware from its issuance in 2016 through its redemption in 2018.

To Dell, that discrepancy represented an opportunity to increase its economic interest in VMware cheaply by buying Class V shares at a discount – all while expropriating value from its own minority stockholders. At first, Dell repurchased billions-of-dollars' worth of Class V shares, increasing its interest in VMware steadily. But to capture the entire, multi-billion-dollar value that the discount between Class V and VMware represented, Dell had to eliminate the tracking stock.

In 2018, Dell devised a transaction to buy up all the remaining Class V shares at a value that still reflected – and therefore allowed Dell to capture – a significant discount to the value of the VMware shares they were designed to track. Dell then crammed that unfair transaction through a special committee rife with conflicts of interests, and an uninformed vote of minority stockholders, by coercively threatening them all with worse alternatives if they did not acquiesce to an unfair deal.

Once the transaction closed in late-2018, in stepped Quinn Emanuel, along with its co-lead class counsel Labaton Sucharow and additional counsel Robbins Geller, Friedman Oster & Tejtel, and Andrews & Springer, to challenge the deal. In doing so, Quinn Emanuel and its co-counsel repeatedly made history. In June 2020, Quinn Emanuel defeated the defendants' motions to dismiss by overcoming Delaware's demanding *MFW* standard, which allows controlling stockholders to evade

liability if they condition transactions from the start on approval by an independent special committee and an uncoerced, fully informed minority-stockholder vote. Few plaintiffs have made it past that stage. From there, Quinn Emanuel aggressively led the charge through fact and expert discovery, uncovering damning evidence against the defendants that it unveiled in a *Daubert* motion undercutting the heart of the defendants' expert case, and a robust, 100-page pretrial brief that persuasively articulated the class's theories of the case.

Ultimately, the defendants and their counsel – which included Wachtell, Williams & Connolly, Skadden, Simpson Thacher, Latham & Watkins, and Alston & Bird – decided on the eve of trial that it was time to settle. And settle they did, agreeing to pay the class $1 billion in cash. According to Institutional Shareholder Services, that $1 billion cash settlement is the largest stockholder settlement in Delaware or any state court's history by nearly $700 million, and the 17th-largest such settlement in U.S. history. *The American Lawyer* named Quinn Emanuel and its co-counsel "Litigators of the Week" for this historic victory, with commentators stressing the settlement's strong deterrent effect on corporate malfeasance. As one law professor explained, "[t]he eyes of the corporate world cannot avoid taking notice of this result."

$173.5 Million Life Science Arbitration Victory

Quinn Emanuel recently won a $173.5 million arbitration award for our clients NantCell, Inc., a wholly-owned subsidiary of ImmunityBio, Inc., and Immunotherapy NANTibody, LLC. The award was issued against Sorrento Therapeutics, Inc. in a hard-fought arbitration proceeding involving complex biotechnology issues that our clients had filed against Sorrento and its Chairman and Chief Executive Officer, Dr. Henry Ji. The dispute involved two Exclusive License Agreements providing for delivery to our clients of antibodies and antibody materials for use in developing cancer therapies. Our clients sought damages arising from allegations of Sorrento's fraud and breach of obligations to provide bargained-for antibodies. The arbitrator issued a final award in the aggregate amount of $173.5 million, finding that Sorrento had breached both license agreements, of which $156.8 million is payable to NantCell and the remainder to NANTibody. In addition, the arbitrator determined our clients are entitled to declaratory relief that both license agreements remain in full force and effect with respect to ImmunityBio's PD-L1 NK cell. Q

Quinn Emanuel Urquhart & Sullivan, LLP Welcomes New Partner Class

Jesse Bernstein

Jesse Bernstein is based in Quinn Emanuel's New York office. He joined the firm in 2015. His practice focuses on complex commercial litigation, with an emphasis on securities fraud and corporate governance actions. He has represented plaintiffs and defendants in class actions and in individual actions involving the Securities Act of 1933, the Securities Exchange Act of 1934, and state blue sky laws. On the plaintiffs' side, for example, he represents some of the world's largest institutional investors in securities opt-out actions alleging violations of state and federal securities laws. On the defense side, he currently represents one of the world's largest drug companies in a securities class action stemming from an alleged price-fixing conspiracy. He graduated from Harvard Law School in 2015.

Marina Boterashvili

Marina Boterashvili is based in the firm's London office and joined Quinn Emanuel in 2015. Prior to joining the firm, she trained at a large international law firm, spending six months in Moscow. After graduating with a degree in Law from the London School of Economics in 2010, Marina went on to obtain an LLM with Distinction from University College London in 2011, with a focus on public international law and dispute resolution. Marina specializes in complex international litigation and arbitration, with an emphasis on civil fraud, asset tracing, and joint venture and shareholder disputes. Her arbitration experience includes acting on arbitrations under the UNCITRAL, ICSID, SCC, LCIA, and ICC Rules.

Emily Kapur

Emily Kapur is based in the firm's Silicon Valley Office. She focuses on complex commercial litigation, particularly cryptocurrency and finance cases featuring the operation of traditional and nascent trading markets. In the cryptocurrency area, she has defended numerous securities litigation matters filed against crypto companies, litigated commercial disputes among cryptocurrency-focused companies in court and arbitration, and advised numerous crypto projects considering securities liability issues. An experienced trial lawyer, she has represented plaintiffs and defendants in state and federal litigation in California, New York, and Delaware, and in numerous arbitration hearings. Emily holds a Ph.D. in Economics and served as an expert witness for high-profile litigation matters prior to joining Quinn Emanuel. Her Ph.D. and law degree are from Stanford.

Owen Roberts

Owen Roberts is based in the firm's New York office. He focuses on federal and state appeals, case-dispositive briefing in trial-level matters, and mid-trial submissions. He regularly practices in federal and state court in both New York and California, where he was previously a member of Quinn Emanuel's Los Angeles office. He graduated magna cum laude from Harvard Law School, where he was the Coordinating & Outreach Chair of the Harvard Law Review, in 2014. Prior to joining the firm in 2017, he clerked for the Honorable Chief Justice Dana Fabe of the Supreme Court of Alaska and the Honorable Judge Katherine Forrest of the United States District Court for the Southern District of New York.

William R. Sears

William R. Sears is based in the firm's Los Angeles office. He re-joined the firm in 2017 following a clerkship for the Honorable Cynthia M. Rufe in the Eastern District of Pennsylvania, and previously worked in the firm's New York office. His practice focuses on antitrust, competition, and class-action litigation. He has represented both plaintiffs and defendants at every stage of litigation and has tried cases in both federal and state court. Prior to joining the firm, he graduated from Columbia Law School, where he won the Greenbaum prize for best oralist in the school's Harlan Fiske Stone moot court competition and served as the Senior Executive Editor of the Columbia Journal of Environmental Law.

Margaret Shyr

Margaret Shyr is based in the firm's Silicon Valley office, having joined the firm in 2014. She obtained a B.S. in Chemical Engineering from M.I.T. in 2003, a Ph.D. in Materials Science and Engineering from the University of Illinois at Urbana-Champaign in 2009, and a J.D. from Northwestern University School of Law in 2014. Margaret is registered to practice before the United States Patent and Trademark Office. Before attending law school, she prosecuted patent applications before the U.S.P.T.O. as a patent agent.

Zach Summers

Zach Summers is based in the firm's Los Angeles office. He re-joined the firm in 2018. He focuses on technology-related litigation, with an emphasis on complex patent trials. Zach has represented clients such as the Broad Institute, VIZIO, Samsung, Google, Motorola, Cree, and Everlight Electronics at trial and in the ITC. Zach was named a "Litigator of the Week" by The American Lawyer's Litigation Daily for his work for the Broad Institute on CRISPR-Cas9. He graduated from Yale Law School in 2007.

quinn emanuel
865 South Figueroa Street, 10th Floor, Los Angeles, California 90017

business litigation report
quinn emanuel urquhart & sullivan, llp

Published by Quinn Emanuel Urquhart & Sullivan, LLP as a service to clients and friends of the firm. It is written by the firm's attorneys. The Noted with Interest section is a digest of articles and other published material. If you would like a copy of anything summarized here, please contact Elizabeth Urquhart at +44 20 7653 2311.

- We are a business litigation firm of more than 900 lawyers — the largest in the world devoted solely to business litigation and arbitration.
- As of January 2023, we have tried over 2,500 cases, winning 86% of them.
- When we represent defendants, our trial experience gets us better settlements or defense verdicts.
- When representing plaintiffs, our lawyers have garnered over $70 billion in judgments and settlements.
- We have won seven 9-figure jury verdicts and four 10-figure jury verdicts.
- We have also obtained fifty-one 9-figure settlements and nineteen 10-figure settlements.

Prior results do not guarantee a similar outcome.

ATLANTA
AUSTIN
BERLIN
BOSTON
BRUSSELS
CHICAGO
DALLAS
DOHA
HAMBURG
HONG KONG
HOUSTON
LONDON
LOS ANGELES
MANNHEIM
MIAMI
MUNICH
NEUILLY-LA DEFENSE
NEW YORK
PARIS
PERTH
RIYADH
SALT LAKE CITY
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STUTTGART
SYDNEY
TOKYO
WASHINGTON, D.C.
ZURICH