Private Data Breach Litigation Comes of Age

I. Overview

Data breaches are every day 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 experienced significant breach events. Given the rise in 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.[1] 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.[2] 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.[3] 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.[4]

Companies face yet another major risk after a 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.[5] Their task was complicated

---

[1] *Cost of a Data Breach Report 2022* at 9-10, IBM (July 2022), https://www.ibm.com/reports/data-breach.

[2] *Id.* at 4, 6.

[3] *Id.* at 5.

[4] *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.

[5] *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").

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).[6]

In this note, we explore 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 in this field.

II. 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.[7]

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.[8] 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."[9] But "a

---

[6] *See In re: T-Mobile Customer Data Sec. Breach Litig.*, No. 4:21-md-03019 (July 22, 2022); *In re: Equifax, Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247 (11th Cir. 2021); *In re: Capital One Customer Data Sec. Breach Litig.*, No. 19-2915 (E.D.Va. Dec. 12, 2021); *In re: Zoom Video Commc'ns, Inc. Privacy Litig.*, No. 20-02155 (N.D. Cal. Oct. 21, 2021); *Perdue v. Hy-Vee, Inc.*, 2021 WL 3081051 (C.D. Ill. July 21, 2021); *In re: Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-md-02583 (Feb. 7, 2022).

[7] *See, e.g.*, *In re: SuperValu, Inc.*, 870 F.3d 763, 772 (8th Cir. 2017) ("At this stage of the litigation, we presume that these general allegations embrace those specific facts that are necessary to support a link between [plaintiff's] fraudulent charges and the data breaches."); *In re: Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 467 (D. Md. 2020) ("While Defendants may ultimately show, after the opportunity for discovery, that the alleged injuries are not caused by their data breach, it is premature to dismiss Plaintiffs' claims on grounds of traceability.").

[8] 578 U.S. 330, 341 (2016).

[9] *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)).

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.[10]

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. Group One – Plaintiffs Who Have Experienced Direct Economic Injuries

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.[11] It is well settled that a "monetary harm," such as an out-of-pocket loss, falls within the "traditional tangible harms" required for standing.[12] 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."[13] 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.[14]

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

---

[10] *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, compl. (Prayer for Relief) ¶ C(i)-(xvi) (N.D. Ga. Sept. 9, 2022).

[11] *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).

[12] *TransUnion*, 141 S. Ct. at 2204.

[13] *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).

[14] *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).

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."[15] 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[16] of how private plaintiffs articulate the injuries and damages they are pursuing to achieve these ends:

- 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.

- 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.

---

[15] *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *9; *TransUnion*, 141 S. Ct. at 2204 (listing traditional intangible harms).

[16] *See, e.g.*, *Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶¶ 10-13, 71-82 (C.D. Cal. Sept. 13, 2022); *Krefting v. OneTouchPoint, Inc.*, No. 2:22-cv-01052, ECF Doc. # 1, compl. ¶¶ 7, 25 (E.D. Wisc. Sept. 12, 2022); *Gutierrez-Torres v. Clinivate, LLC*, No. 2:22-cv-6532, ECF Doc. # 1, compl. ¶¶ 109, 118 (C.D. Cal. Sept. 13, 2022).

- 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.

- 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.

- 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.

- 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.[17]

- 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 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.

[17] 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.

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."[18] 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."[19] 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."[20]

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."[21] 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)."[22] 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.[23]

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."[24] Believing that "[s]uch an inquiry may be appropriate after a proceeding on the merits" but not on a motion

---

[18] 995 F.3d 295, 301 (2d Cir. 2021).

[19] *Id.* at 303.

[20] *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").

[21] 141 S. Ct. at 2210-11.

[22] *Id.* at 2208.

[23] *Id.* at 2209-2213.

[24] *Id.* at 2222 (Thomas, J., dissenting).

to dismiss, they have allowed Group Three plaintiffs to "have the benefit of discovery" before definitively addressing the standing issue.[25]

- *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."[26]

- *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."[27] 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."[28]

- *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."[29] Accordingly, data breach plaintiffs often plead "invasion of privacy" as an example of the "actual and concrete injuries" experienced by Group Three plaintiffs,[30] 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."[31]

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.[32] 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.[33] Absent further clarification by the U.S. Supreme Court in this area, disparate

---

[25] *In re: Blackbaud, Inc. Customer Data Breach Litig.*, 2021 WL 2718439, at *6 n.15 (D.S.C. July 1, 2021).
[26] *Cotter v. Checkers Drive-In Rest., Inc.*, 2021 WL 3773414, at *4 (M.D. Fla. Aug. 25, 2021).
[27] 141 S. Ct. at 2211 n.7.
[28] *In re: Mednax Servs., Inc. Customer Data Sec. Breach Litig.*, --- F. Supp. 3d ----, 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).
[29] 141 S. Ct. at 2204.
[30] *See, e.g.*, *Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶ 13 (C.D. Cal. Sept. 13, 2022).
[31] *Bohnak v. Marsh & McLennan Cos., Inc.*, 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).
[32] *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *9-11; *see also Patterson v. Med. Review Inst. of Am., LLC*, 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.").
[33] *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).

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 more pro-plaintiff.[34]

e. Plaintiffs Are Encountering Standing Difficulties in the Ransomware Context

There is one final standing issue worth noting. In contrast to a typical data breach in which a hacker seeks to extract PI from a system and then use the contents of that data for financial gain (such as fraudulent charges), a ransomware attack involves the use of malicious software (malware) that prevents or limits users from accessing their data or computer system. Often coupled with a threat to eventually publish that data, cybercriminals utilizing ransomware promise to restore access and not make public the data if the target company makes a ransom payment.

Some courts, while recognizing it is "a close question," have concluded that consumers whose data was subject to a ransomware attack have Article III standing.[35] However, both before and after *TransUnion*, most courts that have addressed the issue have held that plaintiffs subject to a ransomware attack cannot establish standing. While fact-dependent, these courts have focused on the intent of the ransomware attacks—which are usually to extract a payment from a business, not to steal PI. The PI is merely a means to an end, not an end itself. Absent evidence of actual misuse (or, at the very least, solid allegations that the stolen data is very likely to be used for fraud or other identity theft), plaintiffs in garden-variety ransomware cases have faced tough sledding in moving past the pleadings stage due to standing defects.[36]

III. Plaintiffs Are Employing a Medley of Creative Claims

a. Federal Law Has Thus Far Played Little Role 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 will meet a similar fate, at least in the near term.

---

[34] Article III standing is only a requirement in federal court. Except in rare circumstances, state courts generally do not require that plaintiffs have Article III standing to maintain their claims. While the vast majority of data breach litigation occurs in federal court, these differences may cause complications where a case is removed. Some commentators have also questioned whether more data breach litigation will occur at the state level in the coming years, as data breach plaintiffs may attempt—through artful pleading—to avoid or minimize standing issues as much as possible.

[35] *Sheffler v. Americold Realty Trust*, 2022 WL 1815505, at *3 (N.D. Ga. Jan. 19, 2022).

[36] *See In re: Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022) (denying standing in ransomware action and collecting cases from federal courts in Pennsylvania, Puerto Rico, and Arizona with similar holdings).

Absent the enactment of the ADPPA or 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"[37]; 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.[38]

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. State Law Claims Provide Private Litigants with a Cornucopia of Options

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).[39] 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.[40] The California Consumer Privacy Act (CCPA) went into effect

---

[37] *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 927 (4th Cir. 2022).

[38] *Allen v. Vertafore, Inc.*, 28 F.4th 613, 617 (5th Cir. 2022); *see also Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 658-59, 671 (E.D. Pa. 2015) (concluding that "privately holding [PI], even in an unsecured manner, does not constitute a 'voluntary disclosure' under the DPPA" where PI was stored unencrypted on laptops that were stolen from company property by an employee), *aff'd*, 739 F. App'x 91 (3d Cir. 2018).

[39] 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.

[40] 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

January 1, 2020.[41] 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.[42] 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[43] 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.[44]

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.[45] 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.[46] While certain aspects of the CCPA have yet to be fully resolved, including the "notice and cure" provision available to defendants,[47] 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.[48]

In addition to the CCPA, data breach plaintiffs may try to utilize a wide array of potentially applicable state consumer protection or unfair competition statutes as the basis for their claims. For example, in one recent data breach class action, plaintiffs pleaded claims under the Maryland Personal Information Protection Act; the Consumer Protection Acts of Maryland, Virginia, and Washington; the Deceptive and/or Unfair Trade Practices Acts of California, Florida, North Carolina, Oklahoma, South Carolina, and Texas; New York General Business Law section 349; the Missouri Merchandising Practices Act; and the California Confidentiality of Medical Information Act.[49] While a smattering of these claims survived a motion to dismiss, most failed due to the lack of a private cause of action, failure by plaintiffs to plausibly allege a violation, no extraterritorial application of the law, application of a safe harbor provision, or the existence of an adequate remedy at law. To the extent that such claims survived, they often duplicated more robust common-law

---

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.

[41] 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.

[42] Cal. Civ. Code § 1798.150(a)(1).

[43] Cal. Civ. Code § 1798.140(o) (Cal. Civ. Code § 1798.140(v) after Jan. 1, 2023).

[44] Cal. Civ. Code § 1798.140(c) (Cal. Civ. Code § 1798.140(d) after Jan. 1, 2023).

[45] *See, e.g.*, *Karter v. Epiq Sys., Inc.*, 2021 WL 4353274, at *2-3 (C.D. Cal. July 16, 2021).

[46] Cal. Civ. Code § 1798.150(a).

[47] Cal. Civ. Code § 1798.150(b).

[48] *California Consumer Privacy Litigation – 2021 Year in Review* at 9, Perkins Coie (Apr. 2022), https://www.perkinscoie.com/images/content/2/5/252535/2022-CCPA-YIR-2021-v2.pdf.

[49] *In re: Mednax Servs.*, 2022 WL 1468057.

claims or provided only for injunctive relief. It remains to be seen whether these general state statutory claims really move the needle with respect to damages obtained in private data breach litigation.

State Common-Law Claims. Private data breach plaintiffs also have a wide array of state common-law claims are 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.[50] 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.[51] 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.[52] 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.[53]

The fate of negligence per se claims varies wildly. Some jurisdictions recognize negligence per se as a theory of liability, but not a separate claim from general negligence.[54] Of the jurisdictions that recognize it as an independent claim, there are variations that "stem from differences in the standards for negligence per se claims under the laws of different states."[55] "Where recognized, a theory of negligence per se permits a plaintiff to establish the traditional negligence elements of duty and breach by providing that a defendant violated a statutory standard of conduct."[56] But many states do not recognize claims for negligence per se based on laws without private rights of action (like HIPPA), and courts have split on whether the FTC Act can support a negligence per se claim in the data breach context.[57]

---

[50] *See, e.g.*, *Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶¶ 113-194 (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).

[51] *See Kitzler v. Nelnet Servicing, LLC*, No. 2:22-cv-06550, ECF Doc. # 1, compl. ¶¶ 45-50 (C.D. Cal. Sept. 13, 2022).

[52] *See id.* ¶¶ 65-70; Krefting *v. OneTouchPoint, Inc.*, No. 2:22-cv-01052, ECF Doc. # 1, compl. ¶ 60 (E.D. Wisc. Sept. 12, 2022).

[53] *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.

[54] *See In re: Rutter's Inc.*, 511 F. Supp. 3d at 531-33.

[55] *In re: Blackbaud*, 567 F. Supp. 3d at 684.

[56] *In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *17.

[57] *See id.*; *see also In re: Blackbaud*, 567 F. Supp. 3d at 683-84 (collecting cases).

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.[58] While some courts have found these defenses to be persuasive at the pleadings stage,[59] data breach plaintiffs have experienced a surprising amount of success with express and implied breach of contract claims.[60] 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.[61]

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.[62] 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."[63] 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.[64] 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.[65]

Unjust enrichment claims. "[F]ederal courts are not uniform in their analyses of unjust enrichment claims in data breach class actions."[66] 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.[67] As a general rule, where

---

[58] *See In re: Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 410 (E.D.Va. 2020) (outlining defenses).

[59] *See, e.g.*, *Sheffler*, 2022 WL 1815505, at *6 (dismissing claim; finding that plaintiff failed to allege facts to allow a plausible inference that a meeting of the minds existed in which defendant intended to bind itself to protect plaintiff's information); *In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *18-20 (finding that plaintiffs failed to plead facts, typically asserted elsewhere, that the defendant implicitly promised to safeguard their PI in the defendant's "privacy policies, codes of conduct, company security practices, and other conduct").

[60] *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.

[61] *See In re: Mednax Servs.*, 2022 WL 1468057, at *13-14 (dismissing implied covenant claim for this reason).

[62] *See id.* at *27-28.

[63] *Purvis*, 563 F. Supp. 3d at 1384.

[64] *Id.* at 1383.

[65] *Id.* at 1378.

[66] *In re: Rutter's Inc.*, 511 F. Supp. 3d at 538.

[67] *Id.*

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.[68] 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).[69] 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).[70]

Privacy claims. Finally, stand-alone tort claims for invasion of privacy or intrusion into private affairs/seclusion have generally faired 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.[71]

IV. 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.[72] Undoubtedly,

---

[68] *See In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *18.

[69] *See In re: Capital One*, 488 F. Supp. 3d at 411-13.

[70] *See In re: Blackbaud*, 567 F. Supp. 3d at 687-88; *In re: Am. Med. Collection Agency*, 2021 WL 5937742, at *18.

[71] *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.

[72] *See In re: StockX Customer Data Sec. Breach Litig.*, 19 F.4th 873, 886-87 (6th Cir. 2021) (affirming district court order compelling arbitration in data breach case filed as putative class action); *Flores-Mendez v. Zoosk, Inc.*, 2022 WL 2967237, at *1-2 (N.D. Cal. July 27, 2022) (denying motion for class certification brought by data breach victims because representative plaintiff agreed to "Terms of Use" containing a class action and jury waiver).

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.

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.

***

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

Robert Schwartz
Email: robertschwartz@quinnemanuel.com
Phone: 213-443-3675

Stephen Broome
Email: stephenbroome@quinnemanuel.com
Phone: 213-443-3285

David Armillei
Email: davidarmillei@quinnemanuel.com
Phone: 213-443-3278

Maia Livengood
Email: maialivengood@quinnemanuel.com
Phone: 202-538-8000

Jennifer Barrett
Email: jenniferbarrett@quinnemanuel.com
Phone: 212-849-7155

October 4, 2022

To hear John Quinn speak further about this topic with a leading plaintiff-side data breach litigator, please visit https://www.law-disrupted.fm/450-million-settlement-data-breach-litigation-comes-of-age/
To view more memoranda, please visit www.quinnemanuel.com/the-firm/publications/
To update information or unsubscribe, please email updates@quinnemanuel.com