California Consumer Privacy Act Litigation
2022 YEAR IN REVIEW

PERKINSCOIE

TABLE OF CONTENTS

INTRODUCTION

Since the California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, several other states have followed suit and passed, or are in the process of implementing, broader consumer privacy legislation. The CCPA regulates any "business" that operates in California and provides consumers in California with greater control over data that companies collect about them. Moreover, Section 1798.150(a)(1) of the CCPA provides a private right of action to "[a]ny consumer whose nonencrypted and nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure" as a result of a business failing to satisfy "the duty to implement and maintain reasonable security procedures and practices." Damages available for the private right of action under Section 1798.150(a)(1) include a statutory amount between $100 and $750 "per consumer per incident or actual damages, whichever is greater," as well as injunctive or declaratory relief and "any other relief the court deems proper."

Further, the California Privacy Rights Act (CPRA) became effective on January 1, 2023, and enforcement will commence on July 1, 2023. The CPRA amends and expands the CCPA, strengthening the privacy rights of California residents and establishing a new government agency for statewide data privacy enforcement called the California Privacy Protection Agency.

Since the CCPA went into effect, Perkins Coie has tracked every CCPA-related filing and closely monitored the litigation environment for emerging trends and important developments in the case law. We use this real-time tracking to help advise clients on risk and develop effective defense strategies for companies facing litigation.

To date, nearly 300 lawsuits have been filed that assert a CCPA claim. These cases span essentially every industry, including biotech, finance, healthcare, and technology. Further, although the majority of the cases were filed in the federal courts in California in previous years, filings in other jurisdictions including Florida, Michigan, and Georgia are trending upwards. In addition, as we anticipated, the number of filings involving data breaches continued to spike in 2022, a significant disparity from what we saw in the first year after the CCPA went into effect.

In 2022, there were a number of notable court rulings and court-approved class settlements. For instance, courts continue to enforce the limits to the CCPA's private right of action despite efforts by the plaintiffs' bar to expand the scope of claims. Also, there have been approximately 28 class settlements that have received or are awaiting final court approval.

Beyond the overview provided in this report, we also monitor filings on a daily basis and provide real-time updates on cases and important industry decisions to clients and key contacts via our *CCPA Litigation Digest*. To receive this weekly email report, please subscribe here. You can also access our CCPA Litigation Tracker, which is updated regularly and will provide you with additional information regarding statistical and legal trends in CCPA litigation.

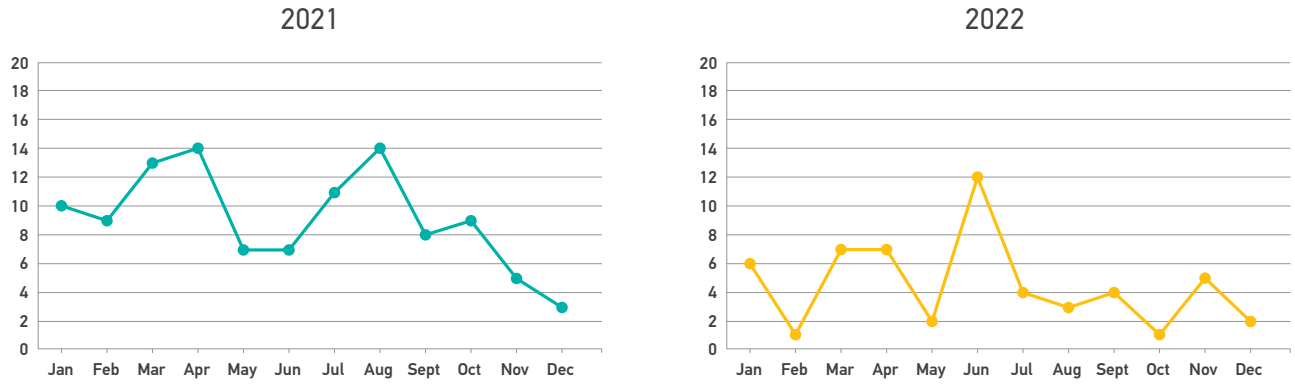
Trends in CCPA Litigation

TOTAL FILINGS

Since the CCPA came into effect in January 2020, nearly 300 cases have been filed by plaintiffs alleging violations of the statute. In 2022, the number of CCPA claim filings remained steady. These lawsuits, nearly all consumer class actions, were filed by approximately 40 different plaintiffs' firms in varying jurisdictions across the country.

TOTAL FILINGS

FIGURE 1

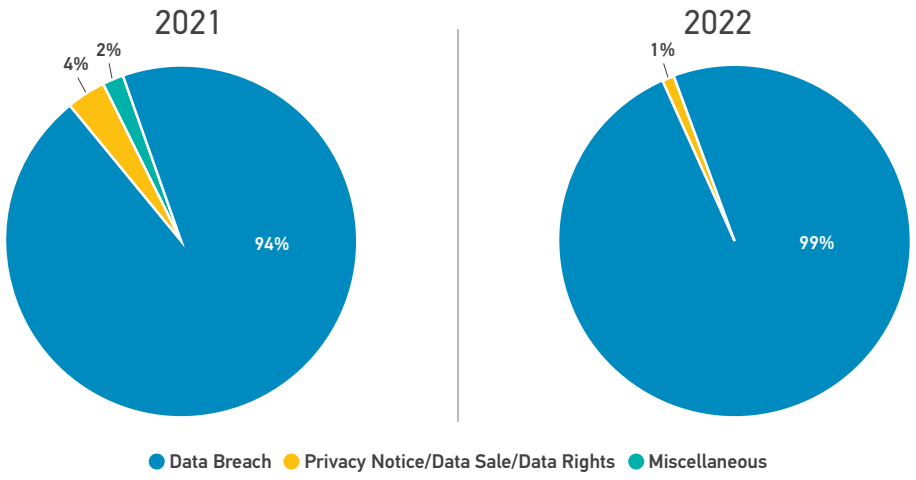


TRIGGERING CONDUCT

An interesting trend we continued to see in 2022 relates to the breadth of conduct that plaintiffs claim gives risk to a CCPA claim. The CCPA does not provide consumers with a private right of action beyond a data breach claim, and thus claims for violations of CCPA privacy rights (e.g., right to notice, right to opt out, right to delete) are not allowed. Notwithstanding this, in 2020, most cases alleging a CCPA claim targeted other conduct addressed by the CCPA, but not included in the private right of action, such as privacy notice, data sale, and data rights. However, in 2021, there was a significant shift wherein 94% of the CCPA claims alleged data breaches without alleging conduct not included in the private right of action. That trend continued in 2022, with over 99% of all CCPA claims focusing on data breaches. This is due in large part to the courts' enforcement, through motions to dismiss and other procedural vehicles, of the limitations on the CCPA's private right of action and the resulting effect of the plaintiffs' bar's increasing reliance on negligence and tort-based privacy claims.

TRIGGERING CONDUCT

FIGURE 2

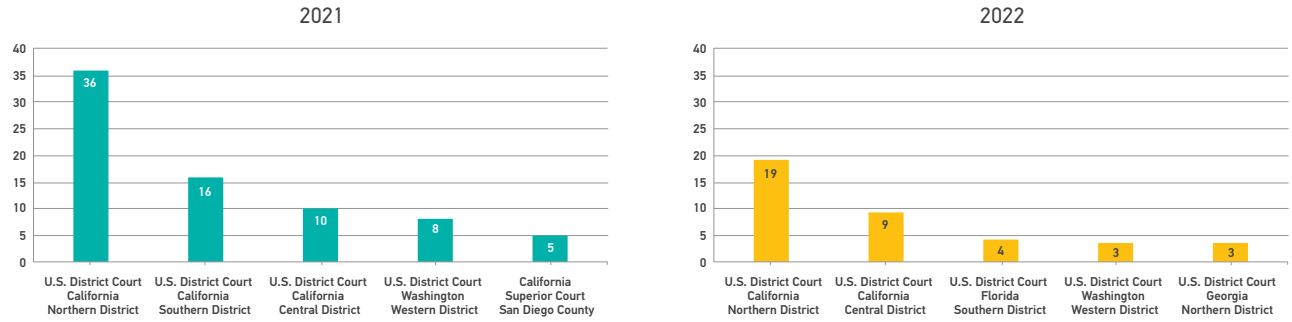


FILINGS BY JURISDICTION (TOP FIVE)

As in the previous two years, the U.S. District Court for the Northern District of California dwarfed all other jurisdictions in the total number of CCPA claim filings in 2022. In fact, more than 35% of all CCPA claims were filed there. The U.S. District Court for the Central District of California had the second most filings. Meanwhile, the U.S. District Courts for the Southern District of Florida and the Eastern District of Michigan made it into the top five jurisdictions with the most CCPA claim filings in 2022.

FILINGS BY JURISDICTION (TOP FIVE)

FIGURE 3

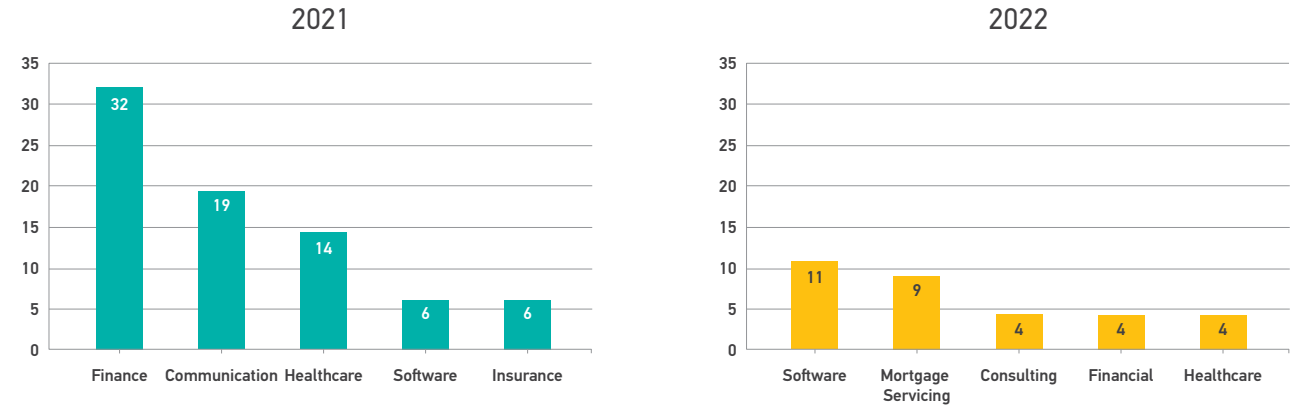


FILINGS BY INDUSTRY (TOP FIVE)

No industry (or company) is immune to a data breach, and consequently, CCPA litigation spanned nearly every industry in 2022. Last year, there was a shift in filings back to the technology/software sector, which had the greatest number of CCPA claim filings, as it did back in 2020. Mortgage servicing/financial and healthcare industries also experienced a significant number of filings.

FILINGS BY INDUSTRY (TOP FIVE)

FIGURE 4



Notable Rulings

NOTABLE RULINGS

LIMITED PRIVATE RIGHT OF ACTION

At the beginning of the year, in *Hayden v. The Retail Equation, Inc., No. 20-cv-01203* (C.D. May 4, 2022), Judge David O. Carter of the U.S. District Court for the Central District of California dismissed a CCPA cause of action because there were no allegations of a data security breach. Judge Carter confirmed what several courts have held to date, that the CCPA's private right of action does not extend to non-data breach violations (e.g., CCPA notice violations). Judge Carter also dismissed the CCPA claim against the retailer defendants because the disclosure of consumers' non-anonymized data was *not* a result of a failure to implement and maintain reasonable security measures but was a business decision to combat retail fraud; thus, § 1798.150(a) was not violated.

ARTICLE III STANDING

The impact upon class-action litigation of the U.S. Supreme Court's decision in *TransUnion LLC v. Ramirez*, including CCPA claims arising from data security incidents, has also been a trending topic in the early stages of CCPA litigation. The last year saw two rulings from the same court with very different results.

In *Wynne v. Audi of America, et al.*, No. 21-cv-08518 (N.D. Cal. Jul 25, 2022), Judge Donna M. Ryu of the U.S. District Court for the Northern District of California denied plaintiff's remand request citing *Spokeo* and *Transunion*. Judge Ryu reasoned that the injury that gives rise to the alleged violation of the CCPA—that is, the "invasion of [Wynne's] privacy interests" that occurred as a result of the theft of her PII (names, home and business addresses, email addresses, driver's license numbers, Social Security numbers, dates of birth, account and loan numbers, and tax identification numbers), is a concrete injury that establishes Article III standing. The court also favorably cited *Al-Ahmed v. Twitter, Inc.*, No. 21-cv-08017 (N.D. Cal. May 20, 2022), which held that "invasion of privacy" resulting from Twitter employees' unauthorized access of Twitter accounts containing private information "is a particularized injury sufficient to establish Article III standing."

However, in *Greenstein v. Noblr Reciprocal Exchange*, No. 21-cv-04537 (N.D. Cal. Dec 5, 2022), Judge Jeffrey White of the U.S. District Court for the Northern District of California dismissed the complaint due to lack of Article III standing. Judge White dismissed the claim for three reasons. First, Judge White held that there was no cognizable threat of future harm for three reasons: the type of personal information (PI) (e.g., driver's license data) did not pose an imminent risk of harm; plaintiffs' PI had not lost value; and plaintiffs' effort and costs attempting to mitigate harm from the breach were insufficient to establish standing because harm is speculative without more sensitive information such as Social Security or routing numbers. Second, no real injury could be traced to defendant's conduct. Third, plaintiffs' alleged harm will not be redressed by a favorable decision e.g., (injunctive or declaratory relief will not compel the hackers or Noblr to return the PI to plaintiffs; and declaratory relief will not motivate Noblr to change its practices since it already took immediate action to change its policy).

Class Settlements

CLASS SETTLEMENTS

To date, there have been 28 class settlements of CCPA claims, either finally approved by courts or in the final approval process. This equates to less than 10% of all the lawsuits asserting a CCPA violation. Despite the early stage and small sample size, there are some significant insights to draw from the class settlements.

SETTLEMENTS OF CASES WITH CCPA CLAIMS ARE LIMITED TO CCPA DATA BREACH CLAIMS

We first note that all of the settled cases involve an alleged data security incident. This may not appear surprising given the CCPA does not provide consumers a private right of action for CCPA violations beyond a limited category of data security incidents. However, plaintiffs in many of the nearly 300 cases filed to date, especially the early filed cases, alleged violations of the CCPA beyond data breach claims. Early court decisions have generally confirmed the CCPA does not extend to non-data breach violations, forcing plaintiffs to narrow their claims.[1] These early rulings appear to have constrained subsequent plaintiffs from attempting to allege claims beyond the scope of the private right of action. As noted above, in 2022, 95% of privacy litigation filed with a CCPA claim involved a data breach. The early settlements appear to follow suit, narrowly resolving data breach claims rather than other CCPA-related claims.

SETTLEMENT VALUES

The monetary relief in the settlements to date encompasses a wide range in total settlement value—from $250,000 to $350 million. The majority of settlements include a non-reversionary settlement fund, while a handful attempt to utilize a claims-made settlement based on out-of-pocket losses with caps. On an individual basis, class settlements range from $0.46 to $244 per class member. Attorneys' fees consistently amounted to 25%-30% of the total settlement value.

EQUITABLE RELIEF CONTAINED IN EACH SETTLEMENT

In addition to monetary relief, all of the approved settlements contained some form of equitable relief (i.e., credit monitoring and/or required data security enhancements).

INCREASED PAYOUT TO CALIFORNIA SUBCLASS

Perhaps the most significant emerging trend is the California settlement subclass. While each settlement contains a nationwide settlement class, some cases also include a California settlement subclass. Members of California subclasses are generally offered additional monetary compensation: often $50 to $100 more than the settlement benefits offered to the nationwide class. These additional payouts for California residents are designed to account for the availability of statutory penalties under the CCPA.

For example, in *In re: Herff Jones Data Breach Litigation*, Case No. 1:21-cv-01329-TWP-DLP (S.D. Ind.), the pending motion for class settlement outlines a cash payment of an extra $100 to the nearly 120,000 Californians notified of a breach. This is specifically related to the statutory penalties available under the CCPA.

CASES FILED OUTSIDE OF CALIFORNIA

In 2022, five of ten settled class actions were filed outside of California. As anticipated, other jurisdictions are interpreting, enforcing, and settling cases involving CCPA claims.

[1] See *McCoy v. Alphabet*, No. 20-cv-05427 (N.D. Cal. Feb. 2, 2021) (a federal district court in San Francisco dismissed a CCPA cause of action because there was no allegation of a security breach); see also, *Silver v. Stripe*, No. 20-cv-08196 (N.D. Cal. Jul 28, 2021) (same federal district court dismissed a CCPA claim based on allegations of improper data sale and disclosure, reaffirming that the CCPA has limited private right of action).

SUMMARY OF THE CCPA SETTLEMENTS TO DATE

Pagan, et al. v. Faneuil, Inc.

Data breach class action alleging logistics and business solutions company failed to protect sensitive personal information of past and present employees as well as mitigate resulting damages. The PII allegedly accessed and stolen included names, addresses at the time of employment, Social Security numbers, and email addresses.

Settlement value: Out-of-Pocket Losses —up to $5,000 per class member; $50 California sub class payment

Class size: 53,476 Nationwide; inc. California subclass of 8,534

Filed: 8.31.22 | **Settled:** 9.1.22

Remoundos, et al. v. LendUS, LLC

Data breach class action alleging mortgage company failed to implement and maintain reasonable security procedures and practices, which led to hackers being able to access employee email accounts, thereby gaining access to personal information of more than 12,000 consumers, in violation of the CCPA.

Settlement value: Out-of-Pocket Losses—up to $2,500 per class member; $100 California subclass payment

Class size: 11,500 Nationwide; California subclass

Filed: 2.4.22 | **Settled:** 6.21.22

In re: T-Mobile Customer Data Security Breach Litigation

Consolidated data breach class actions alleging that telecommunications company exposed the personal information of roughly 50 million current and prospective customers.

Settlement value: $350,000,000

Class size: 76,600,000 Nationwide; includes California subclass

Filed: 12.3.21 | **Settled:** 7.22.22

Lutz v. Electromed, Inc.

Data breach class action alleging medical device company failed to implement and maintain reasonable security procedures and practices, resulting in unauthorized access to customer and employee data, including medical information and health insurance information, Social Security numbers, driver's license numbers, and financial account information.

Settlement value: $825,000

Class size: 47,429 Nationwide; California subclass of 2,966

Filed: 10.6.21 | **Settled:** 10.19.22

Carroll McCallon, et al. v. San Andreas Regional Center

Data breach class action alleging San Andreas Regional Center failed to follow and implement reasonable security practices to protect class members' Protected Health Information (PHI) and PII, resulting in unauthorized access through defendant's remote desktop portal.

Settlement value: $200,000

Class size: Nationwide; California subclass

Filed: 9.16.21 | **Settled:** 5.5.22

James v. Cohnreznick LLP

Data breach class action against accounting firm alleging defendant failed to safeguard employees' PII in connection with a security breach.

Settlement value: Claims-Made Settlement of up to $750 per class member; $100 California subclass payment

Class size: 2,219 Nationwide; California subclass of 248

Filed: 8.2.21 | **Settled:** 1.31.22

Ivo Kolar v. CSI Financial Services, LLC

Data breach class action alleging a provider of patient financing programs to hospitals and health systems nationwide failed to prevent and timely notify patients of an incident in which cybercriminals gained access to the PII and PHI of over 200,000 individuals whose data was stored in its system, which contained patients' names, tax IDs, Social Security numbers, dates of birth, other government-issued IDs, telephone numbers, healthcare account numbers and balances, dates of service, loan numbers and balances, personal banking information, clinical information, health insurance information, and/or photographic images of the patients' faces.

Settlement value: $2,650,000

Class size: 209,664 Nationwide; California subclass of 14,950

Filed: 7.16.21 | **Settled:** 4.22.22

In re: CaptureRX Data Breach Litigation

Data breach class action alleging defendants failed to implement and maintain reasonable safeguards and comply with industry-standard data security practices, resulting in unauthorized disclosure of class members' sensitive medical and personal information, including first names, last names, dates of birth, and prescription information.

Settlement value: $4,750,000

Class size: 2,420,141 Nationwide; California subclass

Filed: 6.2.21 | **Settled:** 2.1.22

Mehta v. Defendant

Putative data breach class action alleging securities trading platform and broker-dealer failed to implement and maintain reasonable security procedures and practices to protect customers' sensitive personal and financial.

Settlement value: Claims-Made Settlement payment of up to $260 ($500,000 cap)

Class size: 40,000 Nationwide

Filed: 2.26.21 | **Settled:** 7.22.22

CCPA Enforcement

CCPA ENFORCEMENT

CALIFORNIA ATTORNEY GENERAL ANNOUNCES FIRST PUBLIC CCPA FINE

As part of his ongoing efforts to enforce the CCPA, Attorney General Rob Bonta alleged that retailer Sephora Inc. failed to disclose to consumers that it was selling their PI, that it failed to process user requests to opt out of sale via user-enabled global privacy controls in violation of the CCPA, and that it did not cure these violations within the 30-day period currently allowed by the CCPA.

The attorney general complained:

- Sephora's online privacy policy falsely stated "we do not sell personal information" despite providing information to advertising and analytics partners.
- Sephora failed to include the required "Do Not Sell My Personal Information" link on its homepage.
- Sephora failed to respond to consumer requests to opt out of such sales via Global Privacy Controls.

On August 24, 2022, Sephora agreed in a settlement to (1) pay $1.2 million into California's Consumer Privacy Fund; (2) make substantial changes to its privacy programs and policies; and (3) submit annual reports regarding these changes to the attorney general for the next two years.

LOOKING AHEAD

As we continue forward, we must remember that the CCPA has been in effect for only three years and many open questions remain. Further, with the addition of the CPRA provisions, we anticipate a steady increase in the number of cases filed involving CCPA/CPRA claims. And as more cases get filed and progress further in litigation, courts will continue to issue notable rulings that will undoubtedly shape the landscape of CCPA/CPRA litigation.

Contact Us

To learn more about issues facing the California Consumer Privacy Act, please contact:

CONTRIBUTORS

DAVID BIDERMAN
PARTNER
LOS ANGELES
+1.310.788.3217
DBiderman@perkinscoie.com

JAMES SNELL
PARTNER
PALO ALTO
+1.650.838.4367
JSnell@perkinscoie.com

SUNITA BALI
PARTNER
SAN FRANCISCO
+1.415.344.7065
SBali@perkinscoie.com

SUSAN FAHRINGER
PARTNER
SEATTLE
+1.206.359.8687
SFahringer@perkinscoie.com

AARON GOLDSTEIN
SENIOR ATTORNEY
LOS ANGELES
+1.310.788.3285
AGoldstein@perkinscoie.com

STEVEN HWANG
SENIOR COUNSEL
LOS ANGELES
+1.310.788.3217
SKHwang@perkinscoie.com

PerkinsCoie.com/Privacy_Security