

# California Court Tosses Alleged “Data Breach” Suit, Holding CCPA Does Not Apply Retroactively

## WRITTEN BY

Timothy J. St. George | Ronald Raether, Jr. | Sadia Mirza | Mary Kate Kamka

---

In *Gardiner v. Walmart, Inc.*, a Walmart customer who purchased goods online filed a putative class action alleging that Walmart’s cybersecurity procedures led to a purported unauthorized disclosure of his personal identifying information (PII).

This purported “data breach” class action is unique in that the plaintiff cannot identify when and how the data breach occurred. Instead, the plaintiff asks the court to assume a data breach occurred because his PII was sold on the dark web.

As a result of this alleged “breach,” the plaintiff brought claims for violation of the California Consumer Privacy Act (CCPA), negligence, violation of California’s Unfair Competition Law (UCL), breach of express and implied contract, and breach of the implied covenant of good faith and fair dealing.

Walmart moved to dismiss all of the plaintiff’s claims and moved to strike the class allegations. While the court dismissed the plaintiff’s claims for the reasons set forth below, it denied Walmart’s motion to strike. The court’s [decision](#) contains key holdings on multiple issues of first impression raised in recent data breach class actions:

### The Bases for Dismissal of the CCPA Claim

The court denied the plaintiff’s attempt to base his CCPA claim on an alleged breach that occurred before January 1, 2020, the date the CCPA became effective. The court held that because the CCPA lacks an explicit retroactivity provision, it cannot apply retroactively under California law. The plaintiff acknowledged that the alleged “breach” occurred after January 1, 2020, but he argued that because his PII is currently being sold on the dark web, the CCPA applies. The court disagreed, and held that a CCPA claim requires a “violation of the duty to implement and maintain reasonable security procedures and practices” that occurred on or after January 1, 2020, which was untrue based on the plaintiff’s allegations.

The court also dismissed the plaintiff’s CCPA claim because he failed to adequately allege the disclosure of “personal information” as defined under the statute. The statute defines “personal information” as a combination of a first name (or initial) and last name and other sensitive PII, such as a Social Security number, driver’s license number, account number, or credit card number with required access codes. See Cal. Civ. Code § 1798.81.5. While the plaintiff generally alleged that his financial and credit card information was accessed, he did not specifically allege the disclosure of the required security codes to access his financial accounts. The court held

that, without such allegations, a CCPA claim cannot stand.

### **The Bases for Dismissal of the UCL Claim**

The plaintiff also alleged his CCPA claim as the predicate violation for his UCL claim. Walmart argued that the plaintiff could not do so because the CCPA expressly prohibits interpreting the statute to “serve as the basis for a private right of action under any other law.” Cal. Civ. Code § 1798.150(c). The court rejected this claim as well, holding that the plaintiff had not established an unlawful practice under the UCL because all of the alleged predicate acts were subject to dismissal.

The court also addressed the plaintiff’s UCL claim by noting that the UCL only provides remedies of restitution or injunctive relief. Monetary damages are not available under the statute. The court found the plaintiff’s purported claims for injunctive relief and restitution unavailing because the plaintiff did not demonstrate any potential future harm, and the plaintiff was not entitled to a refund of his purchase of goods as restitution since there was no dispute that he received the full value goods for which he paid.

### **The Bases for Dismissal of the Negligence Claim**

The court noted that the California economic loss doctrine prohibits claims for purely economic damages under a tort theory unless a “special relationship” exists between the parties. The plaintiff argued that he alleged noneconomic damages in the form of time spent checking his credit and taking preventative measures against identify theft. However, the court held that the value of “lost time” is a form of monetary damage for purposes of the application of the economic loss doctrine. The court further held that no special relationship existed between the plaintiff and Walmart because the transaction at issue was not intended to benefit the plaintiff “in a specific way that sets him apart from all potential Walmart customers.”

### **The Bases for Dismissal of the Contract Claims**

In addressing the contract claim, the court first took judicial notice of various iterations of Walmart’s terms of use (TOU), which contained a disclaimer that information sent or received while using the Walmart website “may not be secure and may be intercepted or otherwise accessed by unauthorized parties.” The TOU further contained a limitation of liability provision that applies to “theft, destruction, unauthorized access to, alteration of, loss of any record or data,” among other things.

The plaintiff argued that Walmart’s TOU was procedurally and substantively unconscionable because it is a contract of adhesion and conflicts with Walmart’s privacy policy. The court rejected this argument, explaining that contracts of adhesion are not *per se* unconscionable under California law, and the TOU was clear enough to enforce its terms and associated limitations. The court then held that because the TOU contained a valid and enforceable limitation of liability clause, the plaintiff’s contract claims were dismissed.

### **The Bases for Dismissal of Plaintiff’s Damages Claims**

Regarding the issue of damages, the plaintiff alleged five different damages theories to support his claims: (1) the improper disclosure of his PII; (2) the future risk of potential fraud and identity theft; (3) the alleged failure to be

notified of the breach; (4) expenses and time spent mitigating the breach's effect; (5) deprivation of the value of his PII; and (6) overpayment for the goods purchased from Walmart.

The court held that each of the plaintiff's theories failed for independent reasons. The claim for "increased risk of identity theft" failed because the plaintiff admitted that he and other class members had closed their financial accounts following the breach. The plaintiff did not explain why his purported costs spent mitigating future effects of the breach were reasonable or necessary. The court further recognized that though a loss in value of PII could potentially support a claim for damages, the plaintiff did not explain why his own PII reduced in value or how that diminishment harmed him. Finally, the court rejected the plaintiff's alleged "overpayment of goods" theory because Walmart never represented in its privacy policy, or otherwise, that it included the cost of data security in the cost of goods.

### **The Court's Denial of Wal-Mart's Motion to Strike Class Allegations**

In addition to seeking the dismissal of the substantive claims against it, Walmart moved to strike the plaintiff's class allegations under both Fed. R. Civ. Proc. 12(f) and Fed. R. Civ. Proc. 23 because some class members agreed to arbitrate their claims in connection with their purchases and provision of PII to Wal-Mart, whereas Wal-Mart contended that the plaintiff did not.

The court denied Walmart's motion under Rule 12(f), holding that Rule 12(f) was not a proper vehicle for dismissing class allegations. The court also denied Walmart's motion to strike class claims under Rule 23 because the record lacked sufficient evidence to establish whether the plaintiff had consented to arbitration. In denying the motion to strike, however, the court acknowledged that "the arbitration issue may prove to be a strong argument against class certification."

### **Procedural Path Forward**

While this decision was favorable to Wal-Mart in numerous regards, the case continues since the court gave the plaintiff leave to amend all his claims. We will continue to monitor this case and similar data breach decisions.

See below for more Troutman Pepper content covering the CCPA:

- [California Consumer Privacy Act Enforcement Series](#)
- [California AG Announces Approval of Fourth Set of Modifications to CCPA Regulations](#)
- [California AG Releases Fourth Set of Proposed Modifications to CCPA Regulations](#)
- [Californians Pass CPRA, Expanding Consumer Privacy Protections](#)
- [California AG Releases Third Set of Proposed Modifications to CCPA Regulations](#)
- [CCPA's Employee and Business-to-Business Information Exemptions Extended Until At Least January 1, 2022](#)

- [The CCPA Regulations Have Been Approved and Are Effective Immediately](#)

## **RELATED INDUSTRIES + PRACTICES**

- [Consumer Financial Services](#)
- [Privacy + Cyber](#)