# First Wave of CCPA Litigation Arrives: How Plaintiffs Are Approaching "Reasonable Security" in Unreasonable Times

**April 24, 2020**

**Jami Mills Vibbert | Alexander S. Altman | Sheena R. Thomas**

The California Consumer Privacy Act (CCPA) provides a private right of action for consumers whose nonencrypted or nonredacted personal information is subject to a data breach as a result of a business's violation of the "duty to implement and maintain reasonable security procedures and practices."[1] Following the CCPA's January 1st effective date, an initial wave of litigation has emerged, testing the contours of the CCPA's private right of action. Most recently, plaintiffs have been targeting a particular strain of CCPA-based litigation and focusing on a cloud-based communications service provider whose services have been increasingly used to facilitate remote work during the COVID-19 pandemic. In all cases, plaintiffs are exploring different paths towards securing a remedy under the CCPA.

In this article, a counterpart to our webinar, we explore the themes emerging from the complaints in this initial wave of CCPA litigation, including cases springing out of circumstances related to the COVID-19 pandemic. We also examine potential defenses to these claims and discuss what it means to maintain "reasonable security procedures and practices," including how businesses can proactively improve their data security postures and strengthen their CCPA compliance programs.

## Relief Under the CCPA and the Origins of the Private Right of Action

The CCPA grants consumers, defined as any natural person who is a California resident, various rights related to the personal information that businesses collect and share about them.[2] Among these rights, the CCPA establishes a limited private right of action following unauthorized access and exfiltration, theft, or disclosure of personal information as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.[3]

The CCPA's private right of action is rooted in the requirements set forth in a California statute that predates the CCPA, the California Customer Records Act (CRA).[4] The CRA requires "[a] business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices."[5] Notably, the CRA codified the concept of "reasonable" security into California law, and specifically allows for customers to institute an action to recover actual damages, but not statutory damages or civil penalties, for a violation of the CRA.[6] Caselaw has established some indications of what is considered reasonable under the CRA. As discussed in further detail below, 2016 guidance published by the California Attorney General provides additional clarity regarding the reasonable security standard and notes that failure to implement all the Center for Internet Security's Critical Security Controls (CSC Controls) that apply to an organization's environment constitutes a lack of reasonable security.[7]

A plaintiff may simply seek injunctive or declaratory relief when bringing a CCPA claim.[8] Plaintiffs may also be entitled to the greater of (1) statutory damages between $100 and $750 per consumer per incident and (2) actual damages.[9] In assessing damages, the CCPA directs courts to consider, inter alia, (1) the nature and seriousness of the misconduct; (2) the number of violations; (3) the persistence of the misconduct; (4) the length of time over which the misconduct occurred; (5) the willfulness of the defendant's misconduct; and (6) the defendant's assets, liabilities, and net worth.[10]

## First Wave of Complaints Filed Under the CCPA

The cases filed under the CCPA so far can broadly be placed in two categories: (1) cases raising claims specifically under the CCPA's private right of action; and (2) "bootstrapping" cases, i.e., cases with claims that bootstrap alleged CCPA violations into a claim under California's unfair competition statute.

### Cases with Claims Arising Under the Private Right of Action

Most of the cases invoking the CCPA thus far are those that include claims under the statutory private right of action. These claims allege: (1) a data breach that resulted from an organization's failure to maintain reasonable security procedures and practices; and/or (2) a separate violation of the provisions in the CCPA that the plaintiffs claim establishes the private right of action.[11] A number of these types of claims have arisen most recently in connection with the increased use of virtual meetings as a result of COVID-19, in which the plaintiffs allege that unauthorized disclosure of personal information as a result of the defendant's violation of the duty to protect personal information.[12]

### Bootstrapping Cases

Other complaints filed thus far do not invoke the CCPA's private right of action but instead, rely on an alleged CCPA violation as the basis for a claim under California's unfair competition law. The California Unfair Competition Law prohibits unlawful, fraudulent, or unfair business acts or practices, as those terms are defined under California law.[13] Plaintiffs allege that violations of the CCPA constitute unlawful activities in contravention of the prohibition on unlawful, unfair, or fraudulent business acts or practices under California law.[14]

## Potential Defenses to CCPA Reasonable Security Claims

While the allegations are nascent, a number of defenses to these CCPA claims—either those asserting the statutory private right of action or bootstrap claims—may be available to defendants in these or similar actions. As of this writing, none of the defendants have yet filed answers to or motions to dismiss the complaints.

### Statutory Standing – The Residency Requirement

The CCPA is clear on who has the standing to bring a claim under the private right of action: a "consumer."[15] Although "consumer" appears to be a fairly generic term, it is defined in the statute to mean only "a natural person who is a California resident[.]"[16] Several of the cases have been brought by individuals who are admittedly not California residents.[17] Any California resident class members could bring these claims, but those non-California residents do not meet the definition of a CCPA consumer. And, named plaintiffs that are residents of California may face difficulties in purporting to represent a multi-state class. Although the CCPA provides that only "consumers" (i.e., California residents) may "institute a civil action," it is silent as to whether class members must also be California residents. Plaintiffs will almost assuredly attempt to broaden class representation as much as possible to leverage larger settlements, but limitations imposed by the Rules Enabling Act and Rule 23 of the Federal Rules of Civil Procedure can be used to resist such attempts.

### Retroactive Application

Another potential deficiency of some of the cases filed thus far is that plaintiffs have alleged breaches or other improper conduct that occurred before January 1, 2020, the effective date of the CCPA.[18] It is unlikely that courts will apply the CCPA retroactively because the text of the CCPA does not expressly allow for retroactive application. The California Supreme Court has held that "[i]t is an established canon of interpretation that statutes are not to be given a retrospective operation unless it is clearly made to appear that such was the legislative intent."[19] Moreover, the CCPA falls under Section 3 of the California Civil

Code, which provides that "[n]o part of [the code] is retroactive, unless expressly so declared."[20] Thus, a defendant may be successful in arguing that it only had a "duty to implement and maintain reasonable security procedures and practices" once the CCPA went into effect on January 1, 2020, and that any alleged breaches occurring before then do not give rise to the CCPA's private right of action.

### Failure to Provide 30- Days' Notice

The CCPA provides that "**prior** to initiating any action against a business for statutory damages. . . a consumer [must] provide[] a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[21] The cases filed have approached this provision in different ways. Some have alleged that notice has been provided without stating when.[22] Some have omitted mention of the notice requirement entirely.[23] A useful analog to the CCPA's notice requirement is the 30-day notice required to bring claims under the California Consumers Legal Remedy Act (CLRA).[24] Courts at both the state and federal level have approved the dismissal of CLRA claims, either with or without leave to amend, for failure to comply with the 30-day notice requirement.[25] In the context of the CCPA, therefore, defendants may have success in achieving dismissal of these complaints, although courts may allow plaintiffs to amend their complaints to attempt to remedy notice requirements.

### Curing Violations Within the Notice Period

The notice provision provides defendants another potential defense: curing the alleged violation. Specifically, if a defendant, within 30 days of notice, "actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur," the action may not be initiated. The criteria for determining whether a violation has been "cured" are unclear, and the statute does not define what it means to cure the violation. One complaint has alleged that plaintiff's notice "demand[ed] that the data breach be cured."[26] Another alleges only that plaintiff sought "a demand for relief" in their notice.[27] None of the Complaints has alleged that the defendants failed to cure their CCPA violations. Therefore, defendants may be able to seek dismissal on the grounds that defendants have not had the opportunity to cure their violations.

While whether a violation has been cured is unclear, defendants may also be able to argue that they did cure the violation as an affirmative defense. That could mean that defendants cured the allegedly unreasonable security measure or it could mean that the defendant remediated any of the alleged harm to the plaintiffs. The CLRA may again prove instructive in that courts have interpreted offers to pay for damages sufficient to satisfy the CLRA's cure provision.[28]

### Alleged Violation is Outside the Scope of the Private Right of Action

Some of the claims brought under the CCPA's statutory right of action raised thus far do not appear to allege a breach of security so much as a failure of a defendant to abide by other requirements of the CCPA, such as the obligation to provide consumers with notice regarding the information to be collected at or before the point of collection or when personal information may be sold to a third party.[29] In these instances, defendants may raise the defense that the alleged violation was not the result of a failure to provide reasonable security, but rather a failure, for example, to provide notice of collection, use, or sale of personal information. This, they will argue, brings the alleged failure outside of the scope of the private right of action, which applies only to "quote statute".

### Proof of Data Breach

The CCPA's private right of action provision has rather unique wording to describe what constitutes an actionable breach: "unauthorized access and exfiltration, theft, or disclosure."[30] In order for a data breach to be actionable, therefore, a plaintiff

will need to prove both (1) unauthorized access to personal information; and (2) exfiltration, theft, or disclosure of the information. This could be a steep hill to climb because the CCPA does not define any of those terms. What is clear, however, is that mere access to personal information will not sustain the private right of action without something more, such as a theft of information. This could prove troublesome for some of the complaints filed thus far. For example, one plaintiff has alleged that the defendant's software wrongfully runs its encryption key servers out of China and that, therefore, "the Chinese government might be able to see" users' personal information.[31] It is unlikely that hypothetical access—without actual exfiltration, theft, or disclosure—will meet the CCPA's standard.

In addition, similar to what has happened under the Confidentiality of Medical Information Act (CMIA) with respect to the burden on plaintiffs to show information was viewed by a third party, defendants may be able to argue that plaintiffs must prove that the information at issue itself (and not just the defendants' systems) was actually disclosed to or stolen by an unauthorized individual. As we have seen in the CMIA cases, this can be very difficult to accomplish.

### Existence of Reasonable Security Procedures and Practices

The CCPA's private right of action does not apply to every single breach of personal information, but only to those resulting from "a violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[32] This raises the possible defense that a breach occurred *in spite of* the implementation of reasonable security. Defendants are likely to raise this defense, especially in cases where sufficient security safeguards were in place to protect the information at issue. Whether a defendant's security practices are reasonable, however, is likely to be a fact-dependent inquiry that likely cannot be determined on a motion to dismiss or early on in litigation.

### Prohibition on Bootstrapping

With respect to "bootstrapped" claims (i.e., claims citing CCPA violations, but arising under other laws, such as the Unfair Competition Law), defendants likely can rely on the CCPA's provision that "[n]othing in [the CCPA] shall be interpreted to serve as the basis for a private right of action under any other law."[33] This would appear to mean that potential plaintiffs cannot bootstrap unfair competition or other non-CCPA claims. In an analogous situation, the California Supreme Court held that a plaintiff could not "plead around" the "absolute bar to relief" set forth in the Unfair Insurance Practices Act "by recasting the cause of action as one for unfair competition."[34] Defendants are sure to attack bootstrapped claims with the CCPA's specific bar on using the Unfair Competition Law to bootstrap CCPA claims.

## How Can You Avoid CCPA Litigation? And What is Reasonable Security and What Are the Best Practices that Support It?

The best protection against CCPA litigation remains not being subject to a data breach under California law. Reviewing and monitoring security practices can help to prevent security incidents from occurring in the first instance. In addition, assuming plaintiffs get beyond the motion to dismiss stage that may succeed as indicated above, being able to show that reasonable security was in place will be critical. Conducting thorough security risk assessments, particularly ones that evaluate the legal risk of not adopting certain safeguards, as opposed to the mere security risk, can and will be critical to succeeding in CCPA litigation.

The CCPA does not define what constitutes "reasonable security procedures and practices," but direction may be gleaned from regulatory enforcement action and guidance. For example, the Federal Trade Commission (FTC) has applied its statutory authority to enjoin "unfair or deceptive" business practices under the FTC Act[35] to enforce data security practices. The FTC pursues enforcement under its deception authority based on companies' alleged noncompliance with their statements or

commitments related to data security. The FTC has also brought enforcement actions under its unfairness authority against companies for engaging in practices that the FTC believes present an unreasonable risk to the security of the personal information of employees, customers, and consumers.

This "reasonableness" standard has been the central component of more than sixty-five FTC settlements with companies in which the FTC has alleged that defendants' security practices were unfair under Section 5 of the FTC Act, even if they were not contrary to public statements and even if there was no financial harm to consumers. Through these settlements, the FTC has emphasized that companies handling consumer information should implement a data security program that contains administrative, technical, and physical safeguards appropriate to the organization's size and complexity, the nature and scope of its activities, the sensitivity of the personal information, and the cost of available tools to improve security and reduce vulnerabilities.[36]

Although FTC complaints, consent orders, and settlements are not binding on courts adjudicating data security-related claims, the FTC has been the most prevalent regulator with respect to articulating what an unreasonable data security practice is. Therefore, when determining how to minimize legal liability under state and federal law requiring "reasonable" or "appropriate" data security, many organizations rely on FTC settlements as instructive as to what a regulator may deem unreasonable.

In the context of the CRA, which also requires businesses to maintain reasonable security, California has already weighed in on what constitutes reasonableness. In 2016, Attorney General Kamala Harris cited the twenty Center for Internet Security's Critical Security Controls (CIS Controls), stating that "[t]he failure to implement all the [CIS] Controls that apply to an organization's environment constitutes a lack of reasonable security." Although this guidance predates the enactment of the CCPA, courts, and regulators may see consideration of the CIS Controls as a benchmark of reasonableness for the purposes of determining liability for alleged CCPA violations.

Finally, many organizations draw upon industry guidance in the form of the International Standards Organization (ISO) 27001 risk management framework and the National Institute of Standards and Technology (NIST) 800-53 for additional direction with respect to reasonable security. ISO 27001 is an international standard providing requirements for an information security management system that is widely used to benchmark and evaluate whether controls are "appropriate technical and organizational measures" required under the EU's General Data Protection Regulation. NIST 800-53 is a set of recommended security controls and assessment procedures directed at federal information systems and organizations and is generally the preeminent industry standard for security in the United States.

The most important thing an organization can do to support reasonable security efforts is to document the process. This includes documenting what steps your organization has taken to secure its systems and data, documentation describing processes and procedures, and documentation around assessments and other mechanisms set up to ensure that the security measures are functioning properly and are updated on a regular interval. Engaging with counsel can help determine what is legally necessary to meet reasonable or adequate security practices under this and other statutes and regulations.

---

[1] Cal. Civ. Code § 1798.150.
[2] *Id.* § 1798.100, *et. seq.*

[3] Other, non-breach, violations of CCPA (e.g., a failure to provide an accurate privacy notice) may result in civil penalties levied by the California Attorney General. *See id.* § 1798.155(b). As explained below, however, these failures do not create a private right of action under the CCPA. We also note that, while consumers have been able to bring suit under the CCPA's private right of action since January 1, 2020, the California Attorney General will not start enforcement of the CCPA's other provisions until July 1, 2020.
[4] *Id.* § 1798.80, *et seq.*
[5] *Id.* § 1798.81.5.
[6] *Id.* § 1798.84(b). The CRA does, however, allow for recovery of civil penalties only for violations of Section 1798.83, which relates to the use of personal information for direct marketing, not unauthorized disclosures resulting from unreasonable security. *Id.* at § 1798.84(c).
[7] Harris, Att'y Gen'l, Cal. Dep't of Justice, California Data Breach Report, https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (Feb. 2016).
[8] Cal. Civ. Code § 1798.150(a)(1)(A).
[9] *Id.* § 1798.150(a)(1)(B).
[10] *Id.* § 1798.150(a)(2).
[11] *See* Compl., *Rahman v. Marriott*, No. 8:20-cv-00654 ¶¶ 65-77 (filed C.D. Cal. April 3, 2020); *see also* Compl., *Llamas v. Truefire, LLC*, No. 8:20-cv-00857 ¶¶ 158-165 (filed M.D. Fla. April 14, 2020).
[12] *See, e.g.*, Compl., *Jimenez v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02591 (filed N.D. Cal. April 14, 2020); Compl., *Kondrat v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02520 (filed N.D. Cal. April 13, 2020).
[13] Cal. Bus. & Prof. Code § 17200 *et seq.*
[14] *See, e.g.*, First Amended Compl., *Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 (filed S.D. Cal. April 7, 2020), at ¶ 5; Compl., *Barnes v. Hanna Andersson, LLC*, No. 3:20-cv-00812 ¶ 9 (filed N.D. Cal. Feb. 03, 2020); Compl., *Hurvitz v. Zoom Video Commc'ns, Inc.*, No. 2:20-cv-3400 ¶¶ 212-218 (filed C.D. Cal. April 13, 2020).
[15] Cal. Civ. Code § 1798.150(a)(1).
[16] *Id.* § 1798.140(g).
[17] *See, e.g.*, Compl., *Fuentes v. Sunshine Behavioral Health Group LLC*, No. 8:20-cv-00487 (filed C.D. Cal. March 10, 2020), at ¶ 5; Compl., *Lopez v. Tandem Diabetes Care, Inc.*, No. 3:20-cv-00723 ¶ 5 (filed S.D. Cal. April 16, 2020); Compl., *Taylor v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02170 ¶ 23 (filed N.D. Cal. March 3, 2020).
[18] Compl., *Fuentes*, No. 8:20-cv-00487 ¶ 2; Compl. *Llamas*, No. 8:20-cv-00857 ¶¶ 36, 160.
[19] *Aetna Cas. & Sur. Co. v. Indus. Accident Comm'n*, 182 P.2d 159, 161 (Cal. 1947) (internal quotations and citations omitted).
[20] Cal. Civ. Code § 3.
[21] Cal. Civ. Code § 1798.150(b) (emphasis added).
[22] *See* Compl., *Fuentes*, No. 8:20-cv-00487 ¶ 212; Compl., *Cullen*, No. 5:20-cv-02155 ¶ 39; Compl., *Jimenez*, No. 5:20-cv-02591 ¶ 161; Compl., *Kondrat*, No. 5:20-cv-02520 ¶ 157; Compl., *Lopez*, No. 3:20-cv-00723 ¶ 219.
[23] *See* Compl., *Barnes*, No. 3:20-cv-00812; Compl., *Almeida*, No. 2:20-cv-00559; Compl., *Fuentes*, No. 8:20-cv-00487; Compl., *Hurvitz*, No. 2:20-cv-3400; Compl., *Johnston v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02376 (filed N.D. Cal. April 8, 2020); Compl., *Llamas*, No. 8:20-cv-00857.
[24] Cal. Civ. Code § 1782(a).
[25] *See, e.g., Breen v. Pruter*, 679 F. App'x 713, 722 (10th Cir. 2017) (affirming dismissal of CLRA claim for failure to provide notice within 30 days of filing claim for damages); *Vy Truong v. eBay, Inc., No. B224828, 2011 WL 3716999, at *3 (Cal. Ct. App. Aug. 24, 2011)* (affirming demurrer without leave to amend). *Cf. Pizana v. SanMedica Int'l LLC*, No. 118CV00644DADSKO, 2019 WL 4747947, at *10 (E.D. Cal. Sept. 30, 2019) (dismissing CLRA claim with leave to amend); *Trabakoolas v. Watts Water Techs., Inc.*, No. 12-cv-01172-YGR, 2012 WL 2792441, at *8 (N.D. Cal. July 9, 2012) (same).
[26] *See* Compl., *Rahman*, No. 8:20-cv-00654 ¶ 77.
[27] Compl. *Kondrat*, No. 5:20-cv-02520 ¶ 157.
[28] *See, e.g., Flores v. Southcoast Auto. Liquidators, Inc.*, 17 Cal. App. 5th 841, 850, 226 Cal. Rptr. 3d 12, 19 (Ct. App. 2017) ("Dealer's reasonable correction offer prevented Flores from maintaining a cause of action for damages under the CLRA[].").
[29] *See, e.g.*, Compl., *Cullen*, No. 5:20-cv-02155 ¶ ¶ 14-21; Compl., *Johnston*, No. 5:20-cv-02376 ¶ ¶33-44.
[30] Cal. Civ. Code § 1798.150(a)(1).
[31] Compl., *Kondrat*, No. 5:20-cv-02520 ¶ 30.
[32] Cal. Civ. Code § 1798.150(a)(1).
[33] *Id.* at § 1798.150(c).
[34] *Manufacturers Life Ins. Co. v. Superior Court* (1995) 10 Cal.4th 257, 283, 41 Cal.Rptr.2d 220, 895 P.2d 56.)
[35] 15 U.S.C. § 45(a).
[36] FTC, Privacy & Data Security Update: 2018 (March 16, 2019), *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.