First Wave of CCPA Litigation Arrives: How Plaintiffs Are Approaching "Reasonable Security"

April 28, 2020

Alexander S. Altman
+1 212.218.2102
asaltman@Venable.com

Sheena R. Thomas
+1 202.344.4688
srthomas@Venable.com

Jami Mills Vibbert
+1 212.370.6288
jvibbert@Venable.com

VENABLE LLP

Speakers

Alexander S. Altman
Associate
+1 212.218.2102
asaltman@Venable,com

Sheena R. Thomas
Associate
+1 202.344.4688
srthomas@Venable.com

Jami Mills Vibbert
Partner
+1 212.370.6288
jvibbert@Venable.com

VENABLE LLP

The California Consumer Privacy Act

Overview of the CCPA, Relief Under the CCPA, and the CCPA's Private Right of Action

VENABLE LLP

Key Concerns

Sweeping Coverage

Definitions cover a broad range of data and data sharing activities

New Rules

Compliance with existing laws does not cover the requirements and scope of the CCPA

Class Action Risks

Private right of action provision creates increased litigation risks

Operational Challenges

Obligations will require new business processes and procedures

VENABLE LLP

Scope of CCPA

Any company that does business in California and meets one or more of these standards:

- Annual gross revenue over $25 million
- Collects or shares personal information annually from 50,000 consumers, households, or devices
- Derives at least 50% of annual revenue from sale of personal information

Obligations and limitations extend to all **personal information** maintained about **consumers**

- Consumer = any natural person who is a **California** resident
- Personal Information = information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with consumer or household

VENABLE LLP

Key Requirements

- Right to request information about practices, and *specific pieces of personal information*
- Right to request deletion
- Opt-out of “sales” of personal information
- Non-discrimination for consumers who exercise rights
- Went into effect on January 1, 2020
  - AG enforcement starting July 1, 2020
  - Private right of action available now

VENABLE LLP

California Attorney General Enforcement

- California Attorney General Enforcement – **July 1, 2020.**
  - Businesses have a 30-day cure period after being notified.
  - Can seek an injunction plus civil penalties of up to $2,500 per violation and up to $7,500 per intentional violation.

Considerations

- No cap on civil penalties.
- Penalties and settlement proceeds placed in state fund.

Rulemaking

- The California Attorney General's Office released an initial draft of proposed regulations in October 2019, a first revision of the regulations on February 10, 2020, and a second revision on March 11, 2020.
- The California Attorney General indicated that it must finalize the regulations by the CCPA's July 1, 2020 enforcement date.

VENABLE LLP

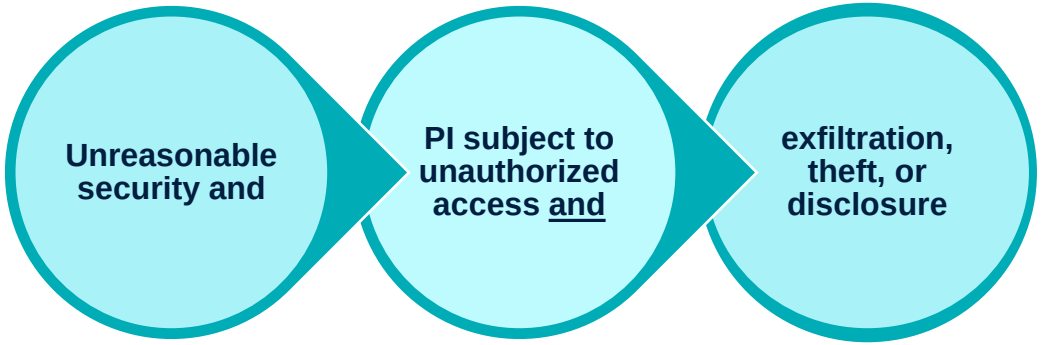
Information Covered

Functional Definition of Personal Information

- Information that:
  - Identifies, relates to, describes,
  - Is capable of being associated with, or
  - Could reasonably be linked, directly or indirectly,
  - *With a particular consumer or household*

VENABLE LLP

Private Right of Action



Encryption and redaction exception

- Different definition of personal information for this section, limited to individual's first name/initial, plus last name, plus:

Social security number	Driver's license or state identification card number	Financial account number, credit or debit card number in combination with access code	Medical information	Health insurance information

- Currently applies to a failure by the business to implement and maintain reasonable security

VENABLE LLP

Private Right of Action: Available Relief

- Greater of:
  - Actual damages and
  - Statutory damages between $100 and $750 per consumer per incident
- Injunctive or declaratory relief
- Any other relief the court deems proper

VENABLE LLP

Private Right of Action: Assessing Statutory Damages

- The nature and seriousness of the misconduct
- The number of violations
- The persistence of the misconduct
- The length of time over which the misconduct occurred
- The willfulness of the defendant's misconduct
- The defendant's assets, liabilities, and net worth

VENABLE LLP

Private Right of Action: Notice and Opportunity to Cure

- Prior to initiating any action for *statutory damages*, consumer must:
  - Provide the business 30 days' written notice.
  - Identify the specific provisions the consumer alleges have been or are being violated.
- No action for statutory damages may be initiated if within the 30 days the business:
  - Actually cures the noticed violation.
  - Provides the consumer an express written statement of cure.
    - But if violations continue after statement, consumer may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.
- Notice is not required prior to an individual consumer initiating an action solely for actual damages or injunctive relief.

VENABLE LLP

Private Right of Action – Scope of Violations

- Applies only to violations that are within the scope of the private right of action (i.e. a breach that is the result of a failure to provide reasonable security).
- Cannot be based on violations of any other section of the statute (e.g., failure to give notice of processing, sale opt-out).
- Bars use of CCPA as basis for a private right of action under any other law.

VENABLE LLP

First Wave of Complaints

Filed Under the CCPA

VENABLE LLP

The First Wave of Cases Filed Under the CCPA: Two Types

1. Cases raising claims specifically under the CCPA's private right of action.

2. "Bootstrapping" cases, i.e., cases with claims that bootstrap alleged CCPA violations into a claim under California's unfair competition statute.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action

- Alleged CCPA Violations:
  - A data breach resulted from an organization's failure to maintain reasonable security procedures and practices; *and/or*
  - A separate violation of the provisions in the CCPA that plaintiffs claim establish the private right of action.

Cases with Claims Arising Under the Statutory Private Right of Action

***Llamas v. Truefire, LLC*, No. 8:20-cv-00857 (filed M.D. Fla. April 14, 2020)**

- Ongoing breach between of August 3, 2019 to January 14, 2020.
- Violation of the duty through defendant's website, defendant's e-commerce platform, and/or from the dark web.
- **Relief Sought:** Actual damages, injunctive or declaratory relief, and other relief the court deems proper, and attorneys' fees and costs; reserve the right to amend complaint to seek statutory damages and other relief under the statute.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action

***Fuentes v. Sunshine Behavioral Health Group LLC*, No. 8:20-cv-00487 (filed C.D. Cal. March 10, 2020)**

- Breach occurred on September 4, 2019.
- Nonencrypted and nonredacted personal and medical information.
- Notice provided.
- **Relief Sought:** Injunctive relief; if defendant fails to respond to notice letter or agree to cure violations, plaintiff will also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the court deems proper.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action

***Lopez v. Tandem Diabetes Care, Inc.*, No. 3:20-cv-00723 (filed S.D. Cal. April 16, 2020)**

- Defendant learned of breach on January 17, 2020.
- Nonencrypted and nonredacted personal and medical information.
- Notice provided.
- **Relief Sought:** Injunctive relief; if defendant fails to respond to notice letter or agree to cure violations, plaintiff will also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the court deems proper.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action: Zoom Cases

***Jimenez v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02591 (filed N.D. Cal. April 14, 2020)**

- Complaint alleges numerous violations of CCPA:
  - Failure to give notice of sharing PI with Facebook.
  - "Zoombombing"
  - Breach leading to publishing of account credentials on the dark web.
- **Relief Sought:** Injunctive relief. Notice was provided to defendant prior to filing of the complaint; reserves right to seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action: Zoom Cases

***Kondrat v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02520 (filed N.D. Cal. April 13, 2020).**

- Complaint alleges numerous violations of CCPA, including:
  - "End-to-end encryption" misstatement; encryption routed through China.
  - Unsecured meeting recordings available online.
  - Meeting chats don't stay private and are not secure.
  - iOS hijacking security flaw.
- **Relief Sought**: Injunctive relief.
- Notice provided – reserves right to seek actual, punitive, and statutory damages, attorneys' fees and costs, and any other relief the Court deems proper.

VENABLE LLP

Cases with Claims Arising Under the Statutory Private Right of Action: Zoom Cases

***Cullen v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02155 (filed N.D. Cal. March 30, 2020)**

- Complaint alleges numerous violations of the CCPA:
  - Collecting and using personal information without providing consumers with adequate notice.
  - Violation of duty to implement and maintain reasonable security procedures and practices.
  - User information sent to FB and possibly other third parties without authorization.
- Notice provided.
- **Relief Sought:** Injunctive relief; if defendant fails to respond to notice letter or agree to cure violations, plaintiff will also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the court deems proper.

Cases with Claims Arising Under the Statutory Private Right of Action: Zoom Cases

***Taylor v. Zoom Video Commc'ns, Inc.*, No. 5:20-cv-02170 (filed N.D. Cal. March 3, 2020)**

- Complaint alleges several CCPA violations:
  - Failure to provide required notice that defendant was disclosing personal information to unauthorized parties such as FB.
  - Failure to provide notice of right to opt-out.
- **Relief Sought:** Injunctive relief and actual damages.

Bootstrapping Cases

- Do not invoke the CCPA's private right of action.
- 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 (Cal. Bus. & Prof. Code § 17200 *et seq*.).
- 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.

VENABLE LLP

Bootstrapping Cases

***Barnes v. Hanna Andersson, LLC*, No. 3:20-cv-00812 (filed N.D. Cal. Feb. 03, 2020)**

- Alleges data breach occurring from September 16, 2019, to November 11, 2019, in which hackers used malware to scrape customer names, contact information, and payment information from the defendant's website.
- **Relief Sought:** In addition to seeking relief under California's unfair competition law, the Complaint states that plaintiff and California class members reserve the right to amend the complaint to seek damages and relief under the CCPA.

VENABLE LLP

Bootstrapping Cases

***Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 (filed S.D. Cal. April 7, 2020)**

- Complaint alleges that defendant collected PI and failed to provide notice at or before the point of collection.
- Complaint asserts that the defendant's unlawful conduct in violation of the CCPA constitutes an unfair practice in violation of California's unfair competition law ("via UCL").
- **Relief Sought:** Restitution, restitutionary disgorgement, injunction, declaratory, and other equitable relief, attorneys' fees and costs.

VENABLE LLP

Bootstrapping Cases

***Hurvitz v. Zoom Video Commc'ns, Inc.*, No. 2:20-cv-3400 (filed C.D. Cal. April 13, 2020)**

- Alleges several security violations among, Zoom, FB, LinkedIn:
  - Zoom security flaws in 2018, 2019 allowing password sharing; AES-128 instead of 256.
  - Improper sharing between Zoom and FB, LinkedIn.
- By omitting, suppressing and concealing that it did not comply with duties pertaining to plaintiff's and class members' personal information under the CCPA, defendant engaged in unlawful, unfair and fraudulent business acts and practices within the meaning of California's unfair competition law.
- **Relief Sought:** Restitution and disgorgement, declaratory and other equitable relief. Plaintiff and class members also assert that they are entitled to injunctive relief.

VENABLE LLP

Potential Defenses

CCPA Reasonable Security Claims

VENABLE LLP

Statutory Standing – The Residency Requirement

- Only “consumers” have standing to bring a claim under the CCPA’s private right of action.
- “Consumer” is defined in the statute to mean only “a natural person who is a California resident[.]”
- Several of the cases have been brought by individuals who are admittedly not California residents. Individuals that are not California residents do not meet the definition of a CCPA consumer.
- Named plaintiffs that are residents of California may face difficulties in purporting to represent a multi-state class.
- The CCPA is silent as to whether class members must also be California residents, but unlikely that courts will extend CCPA relief to non-California residents.

VENABLE LLP

Retroactive Application

- Plaintiffs have alleged breaches or other improper conduct that occurred before January 1, 2020, the effective date of the CCPA.
- 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."
  - 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."
- 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.

VENABLE LLP

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."
- The cases filed have approached this provision in different ways.
  - Some have alleged that notice has been provided without stating when.
  - Some have omitted mention of the notice requirement entirely.
- Analog to the CCPA's notice requirement is the 30-day notice required to bring claims under the California Consumers Legal Remedy Act ("CLRA").
- In the context of the CCPA, defendants may have success in achieving dismissal of these complaints, but note that this notice is only required for statutory damages.

VENABLE LLP

Curing Violations Within the Notice Period

- 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.”
  - Another alleges only that plaintiff stated “a demand for relief” in their notice.
- Defendants may be able to seek dismissal on the grounds that defendants have not had the opportunity to cure their violations.
- Defendants may also be able to argue that they did cure the violation as an affirmative defense.

VENABLE LLP

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

- Some of 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.
- 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 breaches of security that occur "as a result of the business's 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." Cal. Civ. Code § 1798.150.

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."
- 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.
- Similar to what has happened under the Confidentiality of Medical Information Act (CMIA), defendants may be able to argue that plaintiffs must prove that the information at issue itself (and not just defendants' systems) was actually disclosed to or stolen by an unauthorized individual.

VENABLE LLP

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."
- 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.”
- This would appear to mean that potential plaintiffs cannot bootstrap unfair competition or other non-CCPA claims.
- Analogously, 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.”
- Defendants are sure to attack bootstrapped claims with the CCPA’s specific bar on using the Unfair Competition Law to bootstrap CCPA claims.

Recap: Potential Defenses to CCPA Reasonable Security Claims

- Statutory Standing – The Residency Requirement
- Retroactive Application
- Failure to Provide 30-Days' Notice
- Curing Violations Within the Notice Period
- Alleged Violation is Outside the Scope of the Private Right of Action
- Proof of Data Breach
- Existence of Reasonable Security Procedures and Practices
- Prohibition on Bootstrapping

VENABLE LLP

How Can You Prepare for CCPA Litigation?

What is Reasonable Security and What Are the Best Practices that Support It?

VENABLE LLP

How Can You Prepare for CCPA Litigation?

- Avoid being subject to a data breach under California law
- Review and monitor security practices
- If and when a breach occurs, be able to show that reasonable security was in place

VENABLE LLP

What is Reasonable Security?

- The CCPA does not define what constitutes “reasonable security procedures and practices,” but direction may be gleaned from regulatory enforcement action and guidance.
- In the context of the CRA, which also requires businesses to maintain reasonable security, then California 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.”
- Standards for data security have also emerged through case law, agency guidance, regulatory enforcement, self-regulatory standard-setting bodies, and industry best practices.

VENABLE LLP

Reasonable Security Best Practices

Governance	Risk Assessment and Management	Access Controls	Cryptography
Vulnerability Management	Business Continuity and Disaster Recovery	Vendor Management	Security Incident Response Planning

VENABLE LLP

Questions?

VENABLE LLP

VENABLE LLP