CCPA: risk of class actions makes early preparation imperative

Data Protection, Privacy and Security Alert

21 DEC 2018
By: Amanda Fitzsimmons CIPP/US | Jim Halpert

We have previously written about the significant privacy rights afforded to California consumers by the California Consumer Privacy Act (CCPA), a game-changing new law set to go into effect on January 1, 2020 (see our prior reporting on this development here, here and here). But one of the more significant aspects of the CCPA is the major class action litigation risk which the law imposes on those who are bound to comply with its provisions. Preparation is key to mitigating this risk, and the time to begin that preparation is now.

Data breach private right of action

The CCPA contains two sources of class action risk. First, the statute provides a private right of action under certain circumstances to California consumers whose "nonencrypted and nonredacted" personal information[1] is "subject to an unauthorized access and exfiltration, theft, or disclosure 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 information . . . ." Cal. Civ. Code § 1798.150. In other words, the private right of action is available only if the data breach involves *both* "unauthorized access" *and* "unauthorized acquisition theft, or disclosure," *and* it results from the business' violation of the duty to have reasonable security in place in light of the sensitivity of the data that it holds. This means that a notifiable data breach is not actionable unless it involves unauthorized access to the data and it results from unreasonable security.

Significantly, the Act provides such consumers with the ability to obtain relief in the form of either actual damages or statutory damages between $100 and $750 per violation, whichever is greater. *Id.* § 1798.150(a)(1)(A). In setting the statutory damages amount, courts are instructed to consider, among other factors, "the nature, seriousness . . . and persistence of the misconduct," number of violations, "the length of time over which the misconduct occurred," willfulness, and ability to pay. *Id.* § 1798.150(a)(2)(A). In addition to damages, the Act provides for injunctive or declaratory relief and "any other relief the court deems proper." *Id.* § 1798.150(a)(1)(B)-(C).

In order to pursue the private right of action under Section 1798.150, consumers must provide businesses with a 30-day written notice and a 30-day opportunity to cure. *Id.* § 1798.150(b). The consumer cannot initiate an action if, before the 30-day cure period expires, the business provides the consumer with an "express written statement that the violations have been cured and that no further violations shall occur." *Id.* But if the violations continue, the consumer may initiate an action to enforce the express written statement provided to the consumer, and "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." *Id.* Notably, what constitutes a "cure" under the statute is not clear.

The CCPA's provision for statutory damages is significant because it very likely will trigger an increase in data breach class action activity. It:

- arguably allows plaintiffs who have no actual injury to pursue a claim for relief
- creates a pathway to damages in cases where plaintiffs have typically struggled to establish and quantify damages and
- compromises or eliminates several arguments available to defendants opposing class certification, such as the argument that damages cannot be determined on a class-wide basis.

California has a broad data breach notification requirement that is not limited by a risk-of-harm standard, requires notice of larger breaches to the Attorney General and requires the Attorney General to post breach notices it receives on the Attorney General's website.

This private right of action, combined with the broad data breach notice requirement and the availability of statutory damages, makes the CCPA a significant class action risk for companies who are subject to the law.

CCPA as predicate for claims under California's Unfair Competition Law

The second source of potential class action risk comes not from the CCPA on its face, but rather from another California consumer protection statute: the Unfair Competition Law. The UCL is a broadly worded statute that prohibits businesses from engaging in business practices that are "unlawful, unfair or fraudulent." Cal. Bus. & Prof. Code § 17200 et seq. The UCL is a plaintiffs' bar favorite because it allows a plaintiff to "borrow" violations of other laws and treat them as "unlawful" practices for purposes of a UCL claim. *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). The UCL can provide and has provided a pathway for additional relief where a private right of action has been afforded, as well as an independent private right of action where one might not otherwise be afforded under the relevant statute.

However, courts do not permit plaintiffs to utilize statutes as predicates for the unlawful prong of the UCL if the statute expressly precludes such use. Here, there is quite clear evidence that the legislature intended to prohibit such use of the CCPA. Indeed, the first amendments to the data breach section of the CCPA expressly state that the private right of action provided for in the section applies only to data breaches, and on its face, states that consumers may not use the CCPA as a basis for a private right of action under any statute. Cal. Civ. Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.").

Moreover, the CCPA provides the California Attorney General with enforcement authority for violations of other provisions of the Act, which some courts have found is sufficient indicia that the legislature did not intend to permit a private right of action under another law. *See, eg*, *O'Donnell v. Bank of America, Nat. Ass'n*, 2013 WL 98554, at *1 (9th Cir. Jan. 9, 2013) (no private right of action under FTC Act because the Act provided only for enforcement by FTC); *Mordai-Shalal v. Fireman's Fund Ins. Cos.*, 46 Cal. 3d 305, 313 (1988) (holding that delegation of enforcement only to the insurance commissioner was sufficient evidence that the legislature did not contemplate private enforcement).

Nevertheless, California's enterprising plaintiffs' bar is likely to attempt to leverage the CCPA to bring UCL claims. **First,** The CCPA provides for a private right of action for a certain subset of data breaches, and plaintiffs' lawyers will likely argue that plaintiffs may, therefore, pursue UCL claims, e.g. for restitution, using the data breach section of the CCPA as a predicate. In particular, plaintiffs may attempt to sue in state court under the UCL in order to try to avoid federal Article III standing restrictions. **Second,** plaintiffs' lawyers will likely attempt to argue that because the "nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law" clause is found in the data breach section of the law, it should not be interpreted as applying to UCL actions premised upon violations of the other (privacy) sections of the law.

There are strong arguments against both these theories, but businesses should be prepared for plaintiff bar lawsuits that attempt to poke holes in the class action limitation language in the CCPA.

The time to prepare is now

Although the CCPA class action provisions do not take effect until January 1, 2020, compliance with the CCPA takes a significant amount of implementation time and cannot be left to the last minute.

As a start, businesses should consider mapping and understanding data flows of all personal data, including data breach notice data, that is subject to CCPA requirements. Note that the CCPA at this point appears to cover both consumer and employee data, making it important to map both types of data.

With regard to the data elements subject to CCPA class action risk – essentially California data breach notice data minus online account credential data (although credentials can lead to breaches, so should be treated as risky) – companies would do well to be particularly careful as to where those data are located and the security and contractual measures that are in place to manage risk.

These measures may include:

- **Encryption and redaction** -- These are exceptions to breach notice in California. Companies that have these functions in place avoid having to notify of a breach in the first place, thereby greatly reducing risk.Note that encryption should be end-to-end and the encryption keys need to be safeguarded carefully to avoid being obtained in a breach.
- **Valid, truly voluntary class action waivers** – New civil code § 1798.192 of the CCPA purports to invalidate waivers of rights to obtain remedies under the CCPA.However, the Federal Arbitration Act almost certainly preempts this language.The FAA gives class action waivers the potential to be a very effective tool in addressing CCPA class action risk by eliminating a person's ability to pursue class relief for violations, which disincentivizes plaintiffs' law firms from bringing suits in the first place because they are not lucrative.Arbitration also affords companies the added benefits of a private proceeding, less litigation expense, less invasive discovery and the ability to obtain resolution of claims more quickly.However, in order to have a valid arbitration agreement and class action waiver, it is important to have obtained affirmative consent from potentially affected individuals and to use language that meets judicial standards for transparency and voluntariness.
- **Carefully phrased breach notifications** -- If your business suffers a data breach and is sued,the breach notice letter could well be the only evidence before the court at the motion to dismiss phase of the case before discovery.Therefore, to the extent that there are helpful facts that can be included in the breach notice letter, it is worth considering whether to include them in the breach notice letter sent to California residents. In addition, plaintiffs typically pursue claims based on statements a company makes to the public regarding the breach.To the extent that the company is required to or is considering providing written statements regarding an incident, it should include any facts that suggest the breach is not actionable (*eg*, key data elements were not compromised, compromised data elements were redacted or encrypted,)
- **Incident response plan –**Because the CCPA creates new risk associated with many notifiable California data breaches, it is worth considering a review and test of your business' incident response plan in light of the CCPA, paying particular attention to whether it is geared to maximize attorney-client privilege protection in the wake of a suspected breach.
- **Documented Information Security Program -** If the plaintiffs are able to survive a motion to dismiss, eDiscovery will plumb the reasonableness of defendants' information security "procedures and practices." These terms suggest that businesses must have an operational cybersecurity program, not simply written policies and procedures, that conforms with industry standards.Written documentation of the program will serve as favorable

evidence in litigation, as will a certification of adherence to an established security standard.

- **Vendor breach cooperation, security representations and indemnification clause updates** – Increased data breach risk under the CCPA increases the importance of smooth cooperation with vendors and ecosystem partners in the event of a breach. Similarly, greater importance attaches to data security contract representations, security reviews of vendors and clarity as to who bears liability in the event of a breach. Companies should consider adjusting their vendor risk management programs accordingly.
- **Cyberinsurance** – Cyberinsurance typically covers both regulatory actions and class action lawsuits. To the extent that your company is relying on an indemnification clause from a vendor, or provides such indemnities, in light of the size of CCPA statutory damages it is worth determining whether the counterparty has relevant insurance, and the probable coverage in the event of a CCPA-related matter.

Failure to undertake these efforts now could lead to significant liability if a company is breached following the CCPA's January 1, 2020 effective date. It could also lead to potential liability under the UCL if plaintiffs' lawyers are able to convince courts that the UCL can be used as a vehicle to pursue non-data breach related violations of the Act.

Learn more about the implications of the CCPA by contacting either of the authors or your DLA Piper privacy lawyer.

---

[1] For purposes of Section 1798.150, "personal information" is defined as an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (1) social security number, (2) Driver's license number or California ID card number, (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (4) medical information, and/or (5) health insurance information.

AUTHORS

Amanda Fitzsimmons CIPP/US
Partner
San Diego (Downtown) | T: +1 619 699 2700
amanda.fitzsimmons@dlapiper.com

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com