ALSTON & BIRD

WWW.ALSTON.COM

Data Privacy & Security ADVISORY ■

AUGUST 19, 2019

The CCPA Could Reset Data Breach Litigation Risks

By Jim Harvey, Gavin Reinke, and Kaeley Brown

While much has been written about the California Consumer Privacy Act (CCPA), the focus has primarily been on the new rights it affords California consumers to have access to and control use of their data and opt out of many transfers to third parties. While this is a sea change in data privacy legislation in the United States, perhaps the greatest risk to businesses covered by the CCPA is that the CCPA creates a private right of action – with substantial statutory damages – for data breaches. This change will likely reset litigation risks in California in the post-data-breach context and may have significant implications for data breach litigation across the country.

Overview of the CCPA Breach Provisions

The CCPA will do two significant things for the first time in the world of data breach litigation. First, it will give consumers the ability to sue businesses when their "nonencrypted or nonredacted personal information … 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." This private right of action comes into play when the statutory trigger has been met and the incident is a result of the business's failure to implement and maintain "reasonable security procedures and practices." This reasonable security requirement essentially codifies negligence claims found in much of today's post-breach litigation. Second, the CCPA is the first U.S. law to provide for statutory damages in connection with data security incidents, including penalties of $100 to $750 per incident, actual damages, and injunctive relief.

There are two aspects of this portion of the CCPA that provide some hope to breached entities. The definition of personal information used for the private right of action provision of the CCPA is the narrower definition of personal information set forth in the current California data breach notification law, Section 1798.81.5, rather than the now famously broad definition of personal information under the CCPA (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.") The statute also requires both access and exfiltration, theft, or disclosure, which is a more exacting standard than those state breach notification laws that only require unauthorized access to personal data.

Damages: Amount & Factors for Consideration by a Court

The CCPA authorizes courts to award statutory damages in such action of between $100 and $750 "per consumer per incident" or to award actual damages, whichever is greater. *Id.* § 1798.150(a)(1)(A). The statute directs courts to consider a number of factors in assessing the amount of statutory damages to award, "including, but not limited to, 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, and the defendant's assets, liabilities, and net worth." *Id.* § 1798.150(a)(2).[1] These statutory damages are substantial. Moreover, the mere existence of statutory damages will provide data breach plaintiffs with a new argument for standing (which otherwise can be problematic).

First, the statute purports to allow consumers to sue even when they have not suffered any damages as a result of the breach. This is in stark contrast to the most common data breach claims that consumers bring against victims of data breaches today. Those suits are typically based on negligence and/or breach of implied contract theories, both of which require plaintiffs to prove actual damages as an element of their claims. This risk is particularly acute in litigation brought by consumers following the theft of payment card data, where actual damages are often lacking and are difficult to quantify since payment cards are often canceled and reissued after a data breach and financial institutions are generally required to reimburse consumers for unauthorized charges.

Plaintiffs who attempt to allege a violation of the CCPA will still be constrained – at least in federal court – by the constitutional requirement that they suffer a legally cognizable injury-in-fact in order to have standing to sue. This requirement has been difficult to satisfy for plaintiffs in data breach class actions. Moreover, because the U.S. Supreme Court has held that the mere violation of a statute alone is insufficient to confer Article III standing when it is otherwise lacking, the existence of a private-right-of-action provision in the CCPA does not automatically grant plaintiffs the right to bring a claim in federal court. Courts will ultimately need to address the intersection between the CCPA's private-right-of-action provision and Article III standing requirements, and this will be an evolving area of the law that companies should pay close attention to over the next several years.

Second, the amount of statutory damages under the CCPA increases the potential overall exposure companies could face in data breach litigation. The statutory damages, which range from $100 to $750 per incident, can add up very quickly, particularly if a large number of records are impacted by the breach.

Third, the prospect of an award of statutory damages has significant class certification implications if the plaintiffs bring a claim for a violation of the CCPA. Defendants have argued in past data breach cases that individualized damages issues are a significant hurdle to trying the plaintiffs' claims classwide. While the existence of individualized damages issues alone is generally not sufficient to defeat a motion for class certification, it can be part of a powerful argument that predominance is lacking. Thus, in CCPA litigation, defendants will likely have to place a greater emphasis on other defenses to class certification, including case-specific issues that predominate over issues common to the putative class.

---

[1] In order to bring a private right of action under the CCPA, the consumer is required to first "provide[] a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated." Cal. Civ. Code § 1798.150(b).

Reasonable Security Standard

The CCPA's private right of action allows for damages when (1) a company experienced a security incident or data breach; and (2) the company failed to maintain reasonable security practices and procedures. This begs the question of what constitutes "reasonable security." While a detailed discussion of this topic is beyond the scope of this article, potential defendants under the statute should address this issue in their CCPA implementation programs.

In considering this issue, note that California's former attorney general, Senator Kamala Harris, provided quite clear guidance on what she considered reasonable security. In February 2016, the attorney general's office released the California Data Breach Report, which analyzed breaches from 2012 to 2015 and provided guidance on what businesses could consider reasonable security. The guidance focuses on the 20 controls in the Center for Internet Security's (CIS) Critical Security Controls (previously known as the SANS Top 20). According to Attorney General Harris, these controls "identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." While Attorney General Harris's guidance does not have the force of law, it is hard to ignore this guidance for purposes of analyzing these provisions of the CCPA.

Of course, there are a number of other third-party protocols similar to the CIS Controls that one might also assert constitute "reasonable security." These include the National Institute of Standards and Technology Cybersecurity Framework (NIST), which is now well established and in its latest revision has over 900 individual security measures, the Control Objectives for Information and Related Technologies (COBIT) created by ISACA, and the International Organization for Standardization (ISO) ISO/IEC 27000:2018 standards, and many others.[2]

The FTC has also been active in establishing at least what *does not* constitute reasonable security in its eyes. There have been a number of FTC enforcement actions against companies involving security issues, including *In the Matter of Accretive Health Inc.*, Docket No. C-4432; *In the Matter of Uber Technologies Inc.*, Docket No. C-4662; *In the Matter of DSW Inc.*, Docket No. C-4157; *In the Matter of the TJX Companies Inc.*, Docket No. C-4227; *In the Matter of Goal Financial LLC,* Docket No. C-4216; and *In the Matter of Twitter Inc.*, Docket No. C-4316. Of course, there has also been significant litigation in this area somewhat expanding (*FTC v. Wyndham Worldwide Corporation,* 799 F. 3d 236 (3d Cir. 2015)) and contracting (*LABMD Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018)) the FTC's oversight in this area.

Companies subject to existing regulatory regimes have for some time dealt with security standards such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. §§ 160, 164(a), 164(c), and the Gramm–Leach–Bliley (GLB) Safeguards Rule, 15 U.S.C. 6801(b), 6805(b)(2) (among others, although data subject to HIPAA and GLB is currently excepted from application of the CCPA). In the wake of the CCPA, however, companies that have not previously been subject to express regulation of their security

---

[2] A few other states have included similar reasonableness standards in their breach notification statutes (although these statutes do not include corresponding private rights of action). For example, Indiana, I.C. Sec. 24-4.9-3-3.5 (c) (states that "a data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."

practices should now affirmatively consider whether their security programs will allow them to comfortably assert that they have met their "reasonable security" obligation under the CCPA.

National Litigation Implications

Because it includes an express private right of action and authorizes courts to award statutory penalties, the CCPA will substantially increase litigation risk and exposure for companies that are subject to a data breach. The impact will be most strongly felt when claims are brought by (or on behalf of a class of) California residents or against a company that is organized or maintains its principal place of business in California, where the argument for the application of California law will be the strongest. *See Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 821 (1985) (holding that due process is violated when a court attempts to apply the law of one state with "little or no relationship" to the transaction "in order to satisfy the procedural requirement that there be a 'common question of law'"). Nevertheless, the CCPA could have broader implications for data breach litigation nationwide.

First, it could incentivize plaintiffs to file more data breach class actions in California, though plaintiffs will be constrained in their ability to do so by the Supreme Court's decision in *Bristol-Meyers Squibb Co. v. Superior Court*, 137 S. Ct. 827 (2017), which holds that state courts generally cannot exercise personal jurisdiction over an out-of-state defendant for claims brought by nonresident plaintiffs.

Second, plaintiffs' lawyers are also likely to try to effectively expand the scope of the CCPA's private-right-of-action provision by attempting to bring suit or violations of the CCPA under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. That statute prohibits persons or entities from engaging in "any unlawful, unfair or fraudulent business act or practice," and allows plaintiffs to "borrow[] violations of other laws and treat[] them as unlawful practices that the unfair competition law makes independently actionable." *Cel-Tech Communications Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 180 (1999). Plaintiffs are likely to try to argue that *any* violation of the CCPA, regardless of whether it falls within the private-right-of-action provision, is actionable under the Unfair Competition Law. While this has not yet been litigated, companies will have a strong argument that plaintiffs should not be able to evade the narrow scope of the private-right-of-action provision in this manner. The CCPA's private-right-of-action provision expressly states that nothing in the CCPA "shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c). By including this provision in the law, it stands to reason that the legislature expressly intended to exempt the CCPA from the reach of the Unfair Competition Law. Nevertheless, companies should carefully monitor litigation in this area, as a court ruling to the contrary could dramatically increase the litigation risk posed by the CCPA. *See also* Robert D. Phillips, Jr. & Gillian H. Clow, *An Update on the California Consumer Privacy Act and Its Private Right of Action, available at* https://www.alston.com/en/insights/publications/2018/09/california-consumer-privacy-act

You can subscribe to future *Data Privacy & Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Data Privacy & Security Team

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM