Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Privacy Act Will Increase Data Breach Liability

By **Grant Davis-Denny and Alex Gorin** (December 7, 2018, 5:31 PM EST)

Grant Davis-Denny

Alex Gorin

When the California Consumer Privacy Act of 2018, or CCPA, takes effect in 2020, it will usher in not only sweeping new data privacy requirements for businesses, but also a new statutory damages remedy that could significantly increase the importance of data security litigation for companies that conduct significant business in California.

In this piece we examine the statutory damages provision, as part of a series of articles on the CCPA (see "Confusion In Calif. Privacy Act's Anti-Discrimination Rule," "California's Consumer Privacy Act Vs. GDPR," "What Corporate Attys Should Know About Calif. Privacy Act," and "What To Remember About Calif.'s Right To Be Forgotten").

We begin by describing its basic requirements and why it may result in a significant change in businesses' liability exposure for data breaches.

We also assess three questions about the statutory damages provision:

1. Although the provision provides businesses with an opportunity to cure violations, what does this opportunity mean in the context of a data breach?

2. Are statutory damages available when the breach involves a company insider who misuses access privileges?

3. In the absence of a data security breach, is a company that unlawfully discloses data in violation of one of the CCPA's new privacy requirements subject to statutory damages?

Background on the Statutory Damages Provision

The CCPA's statutory damages provision reads in relevant part:

> Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of (1) of subdivision (d) of Section 1798.81.5, 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 personal information may institute a civil action for any of the following: … To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.[1]

One obvious requirement in order for a consumer to recover statutory damages is that the person's data be both "subject to unauthorized access" and to "exfiltration, theft, or disclosure." The CCPA does not, however, define the critical phrase and terms "subject to unauthorized access," "exfiltration," "theft" or "disclosure."

Another key aspect of the statutory damages provision is that stolen personal information can only give rise to liability if the data is not encrypted. Regulated businesses should therefore consider whether some of the sensitive data that they may store or transmit should be encrypted.

The regulated community also should consider that the statutory damages provision's definition of "personal information" is significantly narrower than the definition of that phrase used in other parts of the CCPA. While the CCPA broadly defines "personal information" for most purposes to mean any type of nonpublicly available information that can be linked to a consumer or household (including, for example, names on customer lists and IP addresses), the statutory damages provision uses a more limited definition of "personal information" that is restricted to certain specific categories of information (such as a name and social security number or driver's license number). Businesses subject to the CCPA may want to re-examine how they store or transmit these special categories of data that can give rise to statutory damages liability and whether additional security precautions are warranted.

Consumers can only obtain statutory damages if a business lacks "reasonable security procedures and practices." The CCPA does not attempt to identify what security procedures are "reasonable," and the term obviously leaves much room for debate. We expect that the meaning of "reasonable" security measures will be the subject of substantial litigation and competing expert opinions in the coming years. Again, however, this may provide an opportunity for businesses to take proactive measures now to be better prepared when the CCPA becomes operative in January 2020. Businesses may want to reassess whether their current security procedures and practices satisfy the test of reasonableness given their size, industry, the sensitivity of data collected, and other factors.

Consumers who seek to bring an action for statutory damages must provide two forms of notice. First, a consumer must notify the business 30 days before filing suit of the CCPA provisions that the consumer alleges were violated. If the violation can be cured and the business provides a written statement to the consumer within 30 days that the violation has been cured and no further violation will occur, the consumer then cannot sue for statutory damages (although he or she may sue for actual damages). But if the business violates its written statement, the consumer may then sue to enforce the statement, may recover statutory damages for each breach of the written statement and may obtain statutory damages for "any other violation of the title that postdates the written statement."[2]

The second notice that consumers must provide is to the California attorney general. This notice must be served on the attorney general within 30 days of the suit having been filed. The attorney general can then choose to notify the consumer that the attorney general will be prosecuting an action against the violation (which effectively stays the consumer's case for at least six months), to refrain from acting within 30 days (allowing the consumer's action to proceed), or to notify the consumer that it shall not proceed with the action.[3]

Why the Statutory Damages Provision Could Significantly Change Data Breach Litigation

On an individual basis, statutory damages of $100 to $750 may sound modest. But data breaches often involve the data of millions of consumers. In one high-profile data breach, for example, hackers stole the personal information of 15 million California consumers.[4] If the CCPA had been in effect at the time, the victimized company could have faced statutory damages liability of $1.5 billion to $11 billion. To appreciate what a significant change in liability exposure this represents, consider that the Target data breach resulted in the theft of personal information for 70 million consumers nationwide, but Target reportedly settled class action litigation brought by consumers for only $10 million. In short, the CCPA has the potential to greatly increase damages liability for regulated businesses that suffer a breach involving the personal information of large numbers of California consumers.

What Does the Opportunity to Cure Offer Regulated Businesses?

The obvious scenario that the statutory damages provision was designed to address, and perhaps the only scenario it covers, is one in which an external actor hacks into a company's system, steals sensitive data on California consumers, and then uses, discloses or sells the data. As noted above, under the CCPA, businesses can potentially avoid liability for statutory damages if they cure the defect within 30 days. Specifically, the CCPA states, "In the event a cure is possible, if within the 30 days the business 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, no action for individual statutory damages or class-wide statutory damages may be initiated against the business."[5]

How can a business cure a data breach that results in the theft of data? The CCPA does not provide a ready answer to this critical question. It does not define the term "cure," nor specify what a business must do to be deemed to have cured a violation. A regulated business might contend that it can cure the violation by closing the security gap that led to the breach. But consumers will likely argue that in the event hackers succeed in exfiltrating data, it is too late to cure the violation. We view this as another issue that courts will have to grapple with after the CCPA goes into effect.

Can Statutory Damages Be Recovered When the Attacker is a Company Insider?

Imagine that an IT employee at an online retailer is authorized to access a database containing the personal information of 3 million California consumers. He decides one day to steal the database records from the company's system by downloading them onto a portable hard drive and he takes the storage device to his personal residence. After security software detects the unusual transfer of data to an external storage device, an investigation is launched, law enforcement is contacted and unsuccessful attempts are made to locate the hard drive with the stolen data. Is the company liable for more than $2 billion in statutory damages?

The answer may turn in large part on whether a California court deems the employee's actions "unauthorized access" for purposes of the CCPA, or only unauthorized use. Federal courts have struggled with a similar issue in the context of the Computer Fraud and Abuse Act, or CFAA. In interpreting the CFAA's phrase "accesses … without authorization," some federal courts have drawn a distinction between insider employees who access data to which their employers have not granted them access — which these courts have found to be a violation of the CFAA's "accesses … without authorization" provision — and insider employees who use data to which they have been given access in ways that their employer did not intend — which these courts have found not to be unlawful under the CFAA's unauthorized-access provision.[6] These courts have expressed concern about converting a

general anti-hacking provision into potential criminal liability for employees who merely exceed the use authorized by their employers' computer-use policies.

Although there is a split among the federal circuit courts on this question, at least one California court similarly has distinguished between unauthorized "access" and unauthorized "use" in interpreting a California penal statute that criminalizes accessing a computer without permission.[7] If a California court interpreted the CCPA's "unauthorized access" phrase in the same manner, the employer in our hypothetical would not face statutory damages as a result of its employee's unauthorized use of the data he had authority to access.

It may also be significant that the statutory damages provision does not apply to encrypted data. Because insiders typically have access to consumer data in an unencrypted form, the lack of liability for encrypted data would make little sense if an objective of the statute is to create liability for attacks by insiders with authorized access. Given the conflicting federal precedent, it is reasonable to assume that the applicability of the CCPA's statutory damages provision to certain types of insider breach scenarios will be a subject of significant litigation.

Does the Statutory Damages Provision Apply to Violations of the CCPA's New Privacy Requirements?

Consider a different hypothetical involving the same online retailer. A new privacy provision in the CCPA allows consumers to opt out of allowing a business to sell their personal information.[8] Assume our online retailer has personal information on 750,000 California consumers who exercised their CCPA opt-out rights. The online retailer mistakenly includes those opt-out consumers' data in a data set that the retailer sells to a data broker. Can a plaintiff argue that his or her data was subject to unauthorized access and disclosure when it was improperly sold to the data broker after the plaintiff had submitted an opt-out request to the company? Is the online retailer actually liable for more $500 million in statutory damages?

Probably not, although this too may be the subject of future litigation. As originally enacted, the CCPA revealed a general legislative intent not to create an expansive private right of action. It included a provision that stated that "Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law."[9] CCPA clean-up legislation passed in August further clarified that "The cause of action established by this section [creating the statutory damages remedy] shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other sections of this title."[10] This provision evidences a legislative intent not to apply the statutory damages remedy to any and all violations of the CCPA's new privacy requirements; rather, the remedy is limited to the violations described in the statutory damages provision itself.

A second sign that the statutory damages remedy is limited to data breach scenarios can be found in the statutory damages provision itself. That provision requires that the unauthorized access and theft, exfiltration or disclosure be the "result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[11] The CCPA otherwise does not refer to "reasonable security procedures and practices"; it does not, for example, impose new administrative or technical data security controls on companies. Instead, the CCPA's new requirements are primarily concerned with granting consumers new privacy-based rights to control how their information is stored, used, sold and shared. Yet the statutory damages provision does not refer expressly to any of these new privacy rights.

The CCPA appears to have borrowed the phrase "reasonable security procedure and practices" from a pre-existing California statute, Civil Code section 1798.81.5. That statute requires businesses that own, license or maintain personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The connection between the statutory damages remedy and section 1798.81.5 is further supported by the fact that the CCPA's statutory damages remedy expressly imports the definition of "personal information" used in section 1798.81.5. Unlike the CCPA, section 1798.81.5 is focused on data security, not on data privacy.

It thus seems relatively clear that the CCPA's drafters intended to limit the statutory damages remedy to data breach violations and not to apply generally to violations of the CCPA's privacy provisions.

The California Attorney General appears to have a similar understanding of the CCPA. In a letter urging the Legislature to adopt a broader privacy-based private right of action in CCPA clean-up legislation, the attorney general wrote that "the CCPA does not include a private right of action that would allow consumers to seek legal remedies for themselves to protect their privacy. Instead, the Act includes a provision that gives consumers a limited right to sue if they become a victim of a data breach."[12]

Conclusion

The CCPA's statutory damages provision is likely to generate significant litigation and require California courts to weigh in on various aspects of this important new remedy.

Grant Davis-Denny is a partner and Alex Gorin is an associate at Munger Tolles & Olson LLP.

[1] Civil Code § 1798.150(a)(1).

[2] Civil Code § 1798.150(b)(1).

[3] Civil Code § 1798.150(b)(2), (3).

[4] See California Department of Business Oversight, More Than 15 Million Californians Affected By Equifax Hack (Sept. 13, 2017), available at http://www.dbo.ca.gov/Consumers/alerts/2017/More%20than%2015%20million%20Californians%20affected%20by%20Equifax%20hack.asp.

[5] Civil Code § 1798.150(b)(1).

[6] See, e.g., United States. v. Nosal, 676 F.3d 854, 857-63 (9th Cir. 2012); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); but see United States v. John, 597 F.3d 263, 271-72 (5th Cir. 2010). Note that unlike the CCPA, the CFAA includes provisions that address situations where an individual "exceeds authorized access."

[7] Chrisman v. City of Los Angeles, 155 Cal.App.4th 29, 34 (2007).

[8] Civil Code § 1798.120(a), (c).

[9] Civil Code § 1798.150(c).

[10] Civil Code § 1798.150(c) (as amended by Senate Bill 1121).

[11] Civil Code § 1798.150(a)(1).

[12] Letter from Attorney General Xavier Becerra to The Honorable Ed Chau and The Honorable Robert M. Hertzberg, California Consumer Privacy Act of 2018 (Aug. 22, 2018).