California Consumer Privacy Act: Assessing Your Company's Financial Exposure

Driven by intensifying public concern over the way companies are using consumers' personal information, the State of California recently passed the California Consumer Privacy Act (CCPA). Effective January 1, 2020, the act gives consumers various rights related to the use of their personal information, including rights to know what information businesses are using and how they are using it. It also allows consumers to request that a company delete their personal information or not sell it to third parties.

CCPA Financial Exposure Provisions

Much of the media attention surrounding the CCPA has been focused on the new consumer privacy rights and the need for companies to change their systems and processes to accommodate these rights. For example, the requirement for businesses to provide a clear and conspicuous "Do Not Sell My Personal Information" link on their internet homepages has received significant coverage. However, the act also includes less-publicized provisions that may significantly increase the financial exposure of companies in the event of a data breach or failure to comply with CCPA requirements.

Financial Exposure for Data Breaches

The CCPA gives consumers the right to file a civil lawsuit against a business when the consumer's personal information is compromised in a data breach. These rights apply when the consumer's personal information is:

- "nonencrypted or nonredacted," and
- "subject to 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"

Under these conditions, the act gives consumers the right to recover an amount ranging from **$100** to **$750**, or "actual damages," whichever is greater.

While there is no definition of "actual damages" in the act, presumably, these would be damages for which the consumer would provide some form of documentation or other evidence of financial loss related to the compromise of their personal information.

To determine the appropriate recovery amount within the $100 - $750 range, the court has discretion to consider circumstances associated with the compromised business, including, but not limited to, "the nature and seriousness of the misconduct, the number of violations [of the CCPA], 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."

While the $100 - $750 recovery amount may not seem like a lot, the numbers can add up quickly when a data breach exposes the personal information of a large number of people. In the event of a significant data breach, the recovery rights of all impacted consumers are often aggregated in the form of a class-action lawsuit, which can lead to potentially devastating financial assessments to the breached business. The table below summarizes the potential financial exposure for breaches of varying sizes and court-designated recovery amounts.

	Court-Designated Recovery Amount Per Person		
	$100	***$425***	***$750***
Number of Personal Information Records Breached	**Total Amount Assessed to Breached Business *($ millions)***		
1,000	$0.1	$0.4	$0.8
10,000	$1.0	$4.3	$7.5
100,000	$10.0	$42.5	$75.0
1,000,000	$100.0	$425.0	$750.0
10,000,000	$1,000.0	$4,250.0	$7,500.0

For example, a data breach involving 100,000 personal information records, and for which the court determined that the appropriate recovery amount per person is $425, could result in a **$42.5 million** assessment to the breached business.

Before initiating a lawsuit for recovery of breach-related losses, a consumer, or a representative of a class of consumers, must provide the breached business 30 days' written notice of the CCPA violations that allegedly have been or are being violated. This may include failure to implement and maintain "reasonable security procedures and practices"—more on this later.

If the breached business is able to "cure" the CCPA violation(s) within 30 days of being notified and provides the consumer(s) with a written statement that the violations have been cured and that no further violations shall occur, the consumers will be prevented from initiating a lawsuit. While this might initially appear to allow a breached business to avoid liability by quickly fixing the violations—most likely some form of security failures—the CCPA does not provide any guidance on what an acceptable "cure" would be. One potential—and I believe reasonable—interpretation is that once cybercriminals have accessed personal information, there is no way to "unring the bell," and therefore fixing any security violations after the fact would not provide an acceptable cure.

As with many aspects of the CCPA, there may not be clarity on this issue until the State of California provides further guidance or court cases establish precedent.

Penalties for CCPA Violations

The California Attorney General has the right to assess penalties for failure to cure any alleged CCPA violation within 30 days of being notified of the violation. The penalty amount for intentional violations is $7,500. Non-intentional violations are assessed $2,500. It is not clear whether a violation would have a maximum penalty of either $7,500 or $2,500 for the business as a whole, or if a separate penalty could be assessed for each consumer whose rights were violated. The latter interpretation would, of course, raise the potential financial liability by orders of magnitude. Again, there may not be clarity on this issue until the State of California provides further guidance or court cases establish precedent.

How Can You Protect Yourself?

While there is some lack of clarity regarding the exact level of financial exposure your company may be facing as a result of the CCPA, there is no question that the financial consequences can potentially be devastating. There are three fundamental ways you can mitigate risks of CCPA-related financial impacts:

1. Make sure you have implemented the systems, procedures, and documentation changes needed to support all of the CCPA provisions—for example, putting a "Do Not Sell My Personal Information" link on your homepage.

2. Review your use of personal information and delete, archive, or stop using any of it that is not important for operation of your business. You may be surprised how much personal information you are keeping that is not adding value. It may be appropriate to reduce retention periods of some personal information. In other cases, you may be able to delete it entirely. Cleaning this up is one way to reduce your financial exposure in the event that you are breached.

3. Fortify the security of your environment to ensure you have done everything possible to protect all personal information used in your business. As mentioned earlier, the CCPA requires businesses to implement and maintain "reasonable security procedures and practices." However, the act does not provide any guidance as to what these procedures and practices are. This will likely become clearer over time as the State of California offers clarifications, and court cases establish precedent. In the meantime, there are many existing security standards and best practices that can help you protect personal information.

Tevora's experienced team has the skills and expertise to help you with all three of these areas. We'd welcome the chance to be your trusted partner as you navigate the new and evolving requirements introduced with CCPA.