BLOG

Expect More Class Action Lawsuits after CCPA

By Rob Rosenzweig

Mar 11, 2019

In terms of data privacy regulation, 2018 was a ground-breaking year. On May 25, GDPR, the EU's most stringent regulation on data privacy in 20 years, went into effect, imposing fines of up to €20 million or 4 percent of a company's worldwide revenue for non-compliance. Less than a month later, California passed the strictest data privacy law in the United States with its California Consumer Privacy Act (CCPA).

Now, with the implementation of CCPA less than a year away, (it goes into effect January 1, 2020), anyone doing businesses with California residents should not only be preparing their digital strategies to comply with the new law, they should also be assessing their risk and reviewing their cyber insurance and adequacy of limits.

Why? CCPA establishes a private right of action and statutory damages ranging between $100-$750 per individual per incident. Previously, plaintiffs' attorneys were reluctant to bring an action against organizations experiencing smaller scale incidents as it has been difficult to prove injury in fact and demonstrate actual damages. Now, at $100 minimum per individual incident, a small data breach of 5,000 people equates to $500,000 in damages *at least.*

Given the minimum statutory damage provision, we anticipate that there will be a significant uptick in class action lawsuits following data breaches, even for relatively small breaches.

Data Privacy Law with Real Teeth

CCPA was initiated with the goal of giving Californians control over how their personal data is used, stored and sold. Just like GDPR, it gives Californians the right, among other things, to know what personal information a business is collecting on them, the right to access it, the right to opt-out, the right to delete, the right to know whether it's being sold, and equal access and price regardless of whether or not they're exercising their privacy rights.

The law also defines who the law applies to – namely, anyone who does business in California, whether they're located in California or not. It further defines eligible businesses as having annual gross revenues over $25 million; organizations that buy, receive, sell or share the personal data of 50,000 of more consumers, or that receives 50 percent of its revenue from selling consumers' data.

Changes in Cyber Premiums on the Horizon

As mentioned above, we are almost certainly going to see an uptick in class action litigation once CCPA goes into effect in 2020. Furthermore, the litigation impact is going to move further downstream. The inevitable onslaught of lawsuits could have implications in how cyber insurance is underwritten in terms of pricing and profitability, particularly with the small and middle market.

Prior to CCPA and GDPR, cyber risk carriers had worked under the presumption that middle market clients were unlikely to be hit with lawsuits. The data bore out that assumption.

But, starting in January, as more claims are paid out, premiums could go up. Additionally, many clients historically have based their desired limits on the likely costs associated with the investigation of an incident and the notification of affected individuals. Litigation costs are much more variable and potentially catastrophic. It is important to revisit this decision in the coming months in advance of CCPA's implementation and the onset of similar regulation in other states.

Find me on LinkedIn, here

Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com

Email me directly at rrosenzweig@risk-strategies.com

TAGS:
Cyber Liability