TAG CYBER
LAW JOURNAL
FEBRUARY 2020

TIME TO CHECK YOUR CYBER INSURANCE

Now that the CCPA is in effect, some companies will need to revise their policies.

BY SUSHILA CHANANA, NATE A. GARHART AND TYLER GERKING

The cyber insurance markets are beginning to adapt to the new California Consumer Privacy Act (CCPA), which went into effect on January 1. There is great variation in how cyber insurance policies currently address risks under the CCPA. And further developments are expected as the law begins to impact companies under its jurisdiction—that is, companies that, regardless of their location, are for-profit, collect data from California residents, and either have annual revenue of at least $25 million; or collect, store and/or save the data of at least 50,000 California data subjects; or realize at least half of their revenue from the sale of data.

It is critical that companies subject to the CCPA understand the nuances of cyber insurance policies, and how they may be able to negotiate favorable coverage terms when they buy or renew them this year. But first, a little background.

The CCPA provides rights to California residents whose personal data is collected by a company. For example, consumers have the right to understand what categories of data will be collected (and have already been collected) and what the companies do with that data. They have the right to opt out of the sale of their data, the right to have it deleted, the right to avoid pricing discrimination based on data choices they make, and the right to expect companies that hold their data to protect it.

All of those rights except the right to data security are enforced by the California Attorney General's Office through its investigation and fining powers granted under the act. While the attorney general can impose fines of up to $7,500 per violation of the CCPA, even more significant liability can arise through the private right of action available to consumers whose data is at risk because of a breach where reasonable security measures were not in place.

Specifically, an individual consumer may recover anywhere from $100 to $750 in statutory penalties "per [data breach] incident" if his or her nonencrypted and unredacted personal information was subject to unauthorized access as a result of a business's failure to implement and maintain reasonable security procedures and practices. Thus, the potential liability can be significant in a class action lawsuit. Indeed, because it is unlikely that an individual consumer will file a lawsuit for $750, the true power here lies within the class action realm. If a data breach impacts 1 million consumers, the potential recovery could be up to $750 million.

The Impact on Insurance Policies

A company with California operations buying or renewing its cyber insurance policy at this time should proceed with caution. It should avoid making unfounded assumptions about how the privacy liability and regulatory action aspects of a cyber insurance policy work. These may not cover all claims brought under the CCPA.

First, most cyber insurance policies defend and indemnify insured companies against certain types of regulatory actions. One might assume that an action brought by the California attorney general for an alleged violation of the CCPA would qualify as a covered regulatory action. In many instances, however, the regulatory action coverage is triggered only by a data security breach.

As is evident from the long list of consumer rights under the CCPA set out above, there are many opportunities for a company to violate the CCPA without having suffered a data security breach. If the regulatory action coverage is defined too narrowly, and applies only to regulatory claims arising from a data security breach, the insured company will have no chance of securing reimbursement of defense costs or any settlement or award that doesn't involve a breach. The insurance buyer should seek to expand the agreement to encompass all enforcement actions brought under the CCPA.

Second, even if the regulatory action coverage applies broadly to enforcement arising from privacy violations other than data security breaches, many cyber insurance policies define privacy violation too narrowly. They may not capture some violations that the insured company might be alleged to have committed.

Cyber insurance policies often define this provision with a laundry list of possible infractions based on antiquated conceptions of what privacy rights exist. But the CCPA grants new privacy rights to consumers, which creates the risk of claims based on violations that are not identified in the cyber insurance policy. For example, many policies do not state that coverage includes the right to be free of pricing discrimination. Accordingly, insurance buyers would be wise to either ensure that the laundry list of covered privacy violations includes those identified by the CCPA or, even better, that privacy violation means simply any violation of the CCPA.

Third, cyber insurance policies may exclude coverage for certain fines, penalties and punitive damages, or applicable law may bar insurers from extending such coverage. California law broadly prohibits insurers from covering remedies aimed to punish. Much of the relief that the California attorney general can recover under the CCPA is based on statutory fines. Whether these fines are intended solely to punish a company that violates the CCPA will depend on the circumstances of each particular case. But insurance buyers can strengthen their positions by negotiating a broad choice-of-law clause into the policy that will allow the insurer to cover fines, penalties and punitive damages to the extent permissible under any jurisdiction's laws, or at least any jurisdiction with some connection to the policyholder or the claim. This will give the policyholder (and the insurer) a stronger basis to justify the provision of coverage for a fine imposed under the CCPA.

There is no standard cyber insurance policy, in part because the cyber risk landscape has changed so drastically and unpredictably over the past decade. Each insurer has its own policy language, but most insurers are willing to negotiate the policy terms. As a result, an insurance buyer should not blindly accept whatever policy the insurer offers them. They should closely review the proposed policy to ensure that it addresses their unique risks—and, if it does not, request enhancements. Otherwise, when a claim is received, they may be in for a sore surprise that the policy they bought does not clearly provide the coverage they need and thought they had.

Sushila Chanana *is special counsel at Farella Braun + Martel. She is a high-stakes technology litigator and legal adviser who counsels companies on compliance with various data protection laws, including the CCPA. Her litigation experience includes complex patent, trademark, copyright and trade secrets disputes. Prior to her legal career, Chanana was a cyber security consultant at PricewaterhouseCoopers.*

Nate A. Garhart *is special counsel at the firm and counsels clients on internet issues, online privacy and compliance with laws such as the CCPA and the EU's GDPR. His practice also focuses on maximizing the value of trademark and copyright properties.*

Tyler Gerking *is chair of the firm's insurance recovery group and co-chair of its privacy and cyber security group. He represents corporate policyholders in complex, high-stakes insurance matters. He also helps clients negotiate policy terms, shepherds clients through the claim process, and pursues breach of contract and bad faith claims against insurance companies.*