Privacy and Cybersecurity

Data Breach Lawsuits on Rise

Focus on True Bad Actors Can Prevent Unneeded Litigation

Anyone scanning the headlines these days can see that data breaches have become more prevalent. Cyber criminals are more sophisticated and more aggressive than ever before—even nation states are utilizing this crime as a weapon. This is a complicated and alarming problem in our society that demands thoughtful attention. However, the drastic expansion of civil liability created by the California Consumer Privacy Act (CCPA) in 2018 does not actually address the underlying cyberattacks and will serve primarily to line the pockets of trial lawyers. This expansion of liability also will further harm the very businesses that, despite best efforts, are victims of criminal cyber activity themselves. As a part of the overall policy discussion on amendments to the CCPA, lawmakers also should consider changes to the section regarding civil liability to ensure that it will not turn into another litigation tool that merely extorts costly settlements from California employers.

CALIFORNIA'S ALREADY-EXISTING DATA BREACH LAWS

Civil Code Section 1798.81.5 already requires businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information from unauthorized access, destruction, use, modification, or disclosure." In addition, California already has the strongest data breach notification laws in the country.

Under current law, Civil Code Section 1798.82, businesses are required to report a data breach to California consumers "in the most expedient time possible and without unreasonable delay" even if no harm has been detected whatsoever. (Many states require a showing of harm to trigger their data breach reporting requirement.) Any customer who has been injured by a data breach (due to a violation of Civil Code Section 1798.81.5 or 1798.82) already has a remedy under California's Unfair Competition Law.

CCPA CREATED MASSIVE EXPANSION OF LIABILITY FOR DATA BREACHES

The CCPA created a new, private right of action for "consumers" that does not require a showing of any injury. The CCPA defines a "consumer" as any California resident—so the consumer does not need to have any relationship with a company in order to bring a lawsuit under the CCPA. Moreover, a consumer does not even have to show that his/her data has been stolen in order to file a lawsuit. Under the CCPA, a consumer could bring a lawsuit if his/her personal information was inadvertently disclosed to a vendor. This may seem like the type of lawsuit that wouldn't pass muster, but in the new world under the CCPA where no proof of injury is required, it could succeed—especially given that the definition of personal information is so broad it includes IP addresses, inferences, probabilistic identifiers, and a whole host of other information not traditionally deemed confidential, personal information.

The CCPA imposes a minimum of $100—and a maximum of $750—in statutory damages per person, per incident if a company is found to have failed to maintain reasonable security measures appropriate to the nature of the affected information. Awards of damages under the CCPA will be staggering—enough to put companies out of business. For example, a small business with just 1,000 customers that suffers a data breach could be required to pay up to $750,000 in statutory damages alone. This amount would not even include attorneys' fees or actual damages.

Faced with the risk of such massive damages, companies will be leveraged into immediate settlement —regardless of the

CalChamber

California Promise: Opportunity for All

2019 Business Issues and Legislative Guide

See the entire CalChamber 2019 Business Issues and Legislative Guide at www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsors
Of the 2019 Business Issues and Legislative Guide

Premier

Chevron

Silver

AUTOMOBILE CLUB • SOUTHERN CALIFORNIA • AAA

Bronze

enterprise

Iron

Suburban Water Systems
A SouthWest Water Company

Frontier COMMUNICATIONS

strength of their defense. Thus, the idea that this new law will have an impact only on "bad actors" is simply not true.

The CCPA data breach private right of action is not a stick—it's a sledgehammer. With criminals using bots to relentlessly attack a security system 24/7, they inevitably will succeed in some cases—even where a company utilizes reasonable security measures. Good actor companies that become victims of cybercrime will be pummeled by this new private right of action.

OTHER RECENT LEGISLATION/ACTION PLANNED FOR 2019

• SB 1121 (Dodd; D-Napa)

At the end of the 2018 legislative session, SB 1121 was amended to become the short-term, technical cleanup bill for the CCPA. As introduced, however, SB 1121 proposed a private right of action substantially similar to that created by the CCPA. Only the following proposal from the original SB 1121 did not make it into the CCPA: a private right of action wherein a consumer could bring a lawsuit alleging a business or nonprofit did not notify consumers of a breach in a timely fashion and could recover the significant minimum/maximum statutory damages without any proof of injury. Senator Dodd has indicated he may be reintroducing this proposal in 2019.

• AB 2182 (Levine; D-San Rafael)

After being amended multiple times, the third version of AB 2182 would have dramatically expanded the data breach notification requirements for businesses, mandating that businesses provide rolling notices of data breaches even while the businesses are still determining the full scope of the breaches or working to restore the integrity of the company's data systems. Such a requirement actually would harm consumers by confusing them and it would subject businesses to frivolous lawsuits due to the massive liability businesses now face in the wake of a data breach as a result of the CCPA. The third version of AB 2182 was held in the Senate Rules Committee and did not receive a vote. However, Assembly Member Marc Levine has indicated he may be interested in reintroducing this bill idea in 2019.

POLICY CONCERNS WITH FURTHER EXPANSION OF DATA BREACH LIABILITY

The purpose of data breach notification laws is to provide individuals with clear, accurate and useful information. Mandatory rolling breach notifications would contravene this principle. Specifically, businesses would have to rush to provide notices of a data breach without an understanding of the full picture of what occurred and to whom.

Moreover, it is unclear how often a business would need to notify consumers. Must a business provide an additional notice every day it learns of a new account breached? This lack of clarity coupled with the new requirement would lead to numerous, additional notifications that would not be helpful to consumers. An individual who receives a first notice is likely to disregard subsequent notices. Further, the additional notices could confuse consumers, possibly causing them to take certain actions (some of which cost time and potentially money) that, upon a business's resolution of the breach may turn out to be unnecessary or may not be the best risk mitigation method for that particular situation.

As discussed, the recently adopted CCPA creates massive liability for businesses in the wake of a data breach. Thus, a rolling data breach notification requirement would be a class action magnet, leading to frivolous lawsuits. Trial attorneys would compete to be the first to the courthouse to sue before a company can even assess what has happened. This would take the focus off of bolstering security, reviewing and stopping the extent of the breach, and mitigating risks to the consumer.

CALCHAMBER POSITION

The California Chamber of Commerce will oppose legislation seeking to expand legal liability related to data breach notification. Additionally, CalChamber will support any legislation seeking a safe harbor from data breach liability that would limit frivolous lawsuits for data breaches and encourage companies to utilize elevated security standards.

If the goal of the CCPA's significant liability is for businesses to have solid cybersecurity practices and systems in place, then the Legislature should incentivize such conduct. The Legislature opted for a sledgehammer but should slightly counterbalance that sledgehammer with a small carrot: an affirmative defense for companies with systems and practices that can be certified as in accordance with existing and endorsed security criteria if sued. This will appropriately focus the CCPA's private right of action on the true bad actors and actually address the underlying issue of data security.

Staff Contact
Sarah Boot
Policy Advocate

sarah.boot@calchamber.com
January 2019