"Job Killer" Data Breach Litigation Bill Barely Passes California Senate

Insights
6.01.18

Since my last blog post about SB 1121, the California Senate voted to send SB 1121 to the state Assembly. The May 30 vote was very close, 22-13, only one above the 21-vote threshold for passing the bill and strictly along party lines. Twenty-two Democratic senators voted Yay, 13 Republican senators voted Nay, and four Democratic senators did not cast a vote.

In its current version, SB 1121 risks flooding the courts with data breach lawsuits. According to the Senate Committee on Appropriations May 25, 2018 analysis of fiscal impact, SB 1121 may impose "potentially-significant cost pressures" on the court system, which "could result in delayed court services" for all. This increase in litigation would not necessarily be a reflection of actual grievances and injuries for which victims deserve a remedy; rather, SB 1121 would lower the threshold for when individuals whose private information has been breached can sue businesses. Instead of having to prove that they suffered an injury, under SB 1121, plaintiffs would be able to sue even for a technical breach that did not result in any injury or harm such as identity theft or fraud. Unfortunately, the concept of facing a lawsuit for harmless technical violations is not new to employers in California.

This criticism of SB 1121 has been the subject of a campaign by a diverse coalition of business and industry groups seeking to derail the bill. Have their voices been ignored by the California Senate? Will SB 1121 be amended to address these concerns as it makes its way through the California Assembly?

One glimmer of hope: as the bill was discussed and voted on by Senate, the author of SB 1121 was rumored to be open to amending the bill to create some type of safe harbor whereby businesses could not be sued if they met certain conditions. This chatter may have persuaded some senators to vote for SB 1121 with the expectation that it will be amended to address the "litigation floodgates" concern. For example, Ben Allen (D-Redondo Beach) voted for SB 1121 but expressed interest in adding a safe harbor. A potential amendment may exempt businesses from being sued if they take certain steps to prevent a data breach, such as having updated anti-virus software. This begs the question – do businesses in the 21st century really need a law requiring them to install anti-virus software?

Opponents of SB 1121, who have called it a "job-killer" bill, anxiously await as it moves to the Assembly. Considering the slim margin it passed by in the Senate and the need for a safe harbor that

Assembly. Considering the slim margin it passed by in the Senate and the need for a safe harbor that has been discussed with the bill's author, the hope is that the bill will be amended in the Assembly or be defeated altogether. But even if SB 1121 is amended to include a safe harbor, will this be sufficient to address legitimate concerns about impacting everyone's access to the courts and subjecting businesses to victimless litigation?

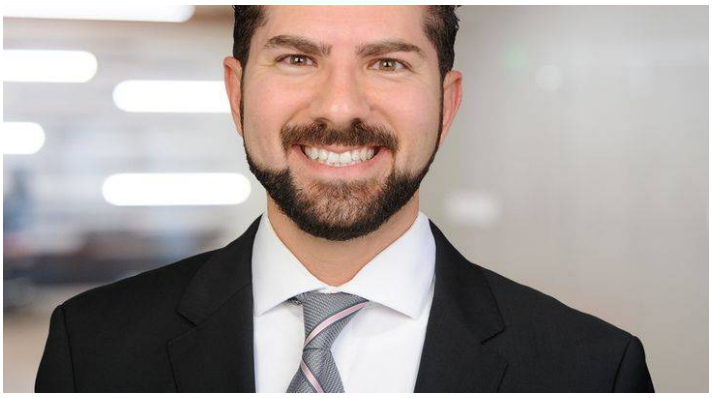
By focusing too much on the rhetoric of consumer protection and data breach prevention (all noble causes and policy objectives), proponents of this bill may be ignoring parts of the broad array of security incidents that may fall within the definition of a "data breach" under the statute. This would result in unintended consequences that seem unfair and unjust.

For example, imagine your payroll representative accidentally sends W2s or other personal information containing SSNs or other sensitive data to the wrong company email list – let's say it goes out to all employees when it should have been sent to a particular group. All the recipients are company email accounts. Some of the recipients open up the emails and view the personal information of their coworkers. Your IT department immediately goes into the email server and deletes all of those emails so they would disappear from each employee's mailbox. IT also confirms that no one has emailed or forwarded the information outside your company, and that only a handful of employees have actually read the email and opened the attachments before deletion. Further interviews with employees who opened the files confirm that none of them printed or shared the information with anyone. At this point, no one outside the company has seen the information and it is no longer accessible to anyone who accidentally received it, and you have no reason to believe there is any risk of harm or identity theft to anyone.

Would this be a data breach under the proposed California law? Attorneys may disagree on the answer, but let's assume the answer is yes. Under SB 1121, all employees of this company would be able to bring a class action against the company and obtain a minimum of $200 per person in damages regardless of whether they were harmed in any way. Adding a safe harbor like having updated anti-virus software is entirely irrelevant to a scenario like this one (which is more common than you think), as anti-virus software would not have made a difference. But let's say your company didn't have anti-virus software installed or didn't have the latest update; SB 1121 would automatically subject the company to liability despite the fact that no one was injured and there is no ongoing risk of harm as the data had already been retrieved.

Employers who are concerned about SB 1121 moving through the California Legislature should consider investing in political advocacy efforts to educate legislators about the perhaps unintended consequences of this bill.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email