Another Federal and Industry Push to Weaken State Data Breach Notification Laws

March 4, 2014 - Ever since the Target data breach late last year, there have been rumblings coming out of Washington, DC about the adoption of a federal standard for data breach notifications. The idea is for congress to write a new one-size-fits-all law that would usurp and replace all of the state data breach laws currently on the books. It is an argument that sounds goodâ€¦ right up until you start to examine the details associated with every single federal proposal so far. Once you do that, it becomes fairly easy to see why retailers love the idea, and why it should make most consumers very nervous.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Ever since California passed the nation's first - and arguably the toughest - data breach law, a wide variety of interests have been asking congress for a national data breach law. It should be no surprise that the national laws proposed have been riddled with notification loophole and reduced penalties. To date, congress hasn't been able to muster the votes to pass such a law. That's something that we should all be thankful for but which may be about to change.

The Target data breach and its massive scope have made the issue something which is attractive to lawmakers. After all, data security really shouldn't be a partisan issue. And just this week, Attorney General Eric Holder publically called for a national standard for data breach notification. That call is likely to give some momentum to this latest push.

There are now two separate proposals floating around the halls of congress for a national law. And as with previous proposals, both would weaken laws already on the books. They do this by only requiring notification if the party experiencing the breach has a "reasonable suspicion" that the stolen data will be used for fraud or ID theft. And they leave the job of determining what is "reasonable" up to the party who caused the data breach in the first place.

Contrast that with California's law. California also includes "reasonable suspicion" in its law. But there is a big difference. The California law requires notification if the party holding consumer data has a "reasonable suspicion" that the data has been stolen or breached. It doesn't matter if they think someone will use the data for illegal purposes. Only that they think there may have been a data breach.

Frankly, most companies wouldn't support a national standard that conforms to California law. But you are unlikely to hear your congressional delegation, the White House, or anyone who controls databases containing large amounts of consumer data say that. In fact, they are much more likely to frame the conversation in such a way that it makes you think they want stronger laws. Simply stated, that's a farce.

Consumers need to be aware of this issue and the pending legislation being considered. Making sure that your congressional delegation understands that you have no interest in weakening existing data breach notification laws is likely the only way to strengthen the current proposals, or to get congress to drop this idea entirely.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS