White House and Congress Pushing for National Data Breach Notification Law

February 12, 2015 â€“ For several years now, various special interests and politicians have been pushing the concept of a national data breach notification standard. On its face, the idea sounds great. But with a closer look at these proposals, it doesnâ€™t take long to figure out that these proposals would significantly reduce the consumer protections that are already in place in many states. The latest proposals coming out of Washington, DC are no exception.

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);
})();

Data breach notification laws started in California and quickly swept across the nation. Today, there are only three states which donâ€™t have a data breach law on the books; Alabama, New Mexico and South Dakota. These three states account for less than 3% of the US population according to the latest census numbers.

Every proposed national data breach law that we are aware of has two things in common. First, all of them would make it illegal for the states to enforce their own data breach laws. Second, all of them are weaker than Californiaâ€™s law; still considered to be the gold standard among such laws.

Congress has already started hearings on President Obamaâ€™s latest proposal for a national data breach standard. And they are already getting pushback from retailers about a proposed requirement that victims be notified of a data breach within 30 days of discovery. Instead, it has been suggested that companies involved in a breach be given a period of time to conduct a risk assessment and, only after that assessment is completed, the 30 day clock for notification should begin. That suggestion is more than a little problematic.

It could take companies months to complete such an assessment. That means that it would be months before any

consumer notifications take place. And in that time, consumers could easily fall victim to fraud and identity theft. Had a law like this been in place when the Target data breach took place there is almost no doubt that more consumers would have been victimized.

The â€œrisk assessmentâ€• proposal is also troubling in that it almost certainly means the proposed law would allow companies to make their own determination about whether or not it is likely that breached data will be used to commit fraud. If the determination is made that the risk is low, the company would likely face no notification requirement at all. NOTE: The reason we suspect this will be a part of the proposal is that it has been proposed before at a national level. And 18 of the current state notification laws on the books include this loophole.

Another issue with the Presidentâ€™s proposal is that its definition of a data breach doesnâ€™t cover medical records. That is simply poor planning. Medical records have become significantly more valuable to hackers than credit card and financial data. In fact, medical records can fetch prices that are 40 or 50 times higher on the black market than simple financial records.

Again, the California law comes into play. Californiaâ€™s data breach law includes medical records. The proposed federal law, in its current form, would make it illegal for California to require companies to make a data breach notification when medical records are breached.

Unfortunately, the push is on for what could become a weak national law dealing with data breaches. According to an article in the Credit Union Times, a representative from the National Retail Associatio, had the Gaul to tell congress that â€œcompanies would improve their data security if Congress required them to meet uniform notification standards in the event of a data breach.â€•

The article quotes him as saying â€œâ€™Congress needs to provide incentives for companies to increase their security and nothing motivates like sunlight, requiring that every company have the same public notice obligations will provide this needed light.â€™â€•

In our opinion, they appear to be telling congress that unless a national law is passed, they arenâ€™t going to make a sincere effort to protect consumer data. Of course if a weak bill does become law, they may not have to do anything additional to protect consumers. Consumers are simply caught in the middle.

Weâ€™ll continue to keep you posted as the bill moves through congress.
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