SpencerFane®

Updated Proposed Federal 30-day "Shot Clock" For Data Breach Notification

JANUARY 13, 2015| PUBLICATIONS

As we wrote yesterday, President Obama has called for legislation (the Personal Data Protection and Privacy Act) that will require notice of a data breach within 30 days of discovery by your company.

The a Wall Street Journal is reporting that the proposed legislation and a national standard for notification does have support from the National Retail Federation, but the NRF does not believe a set timeline of 30 days is practical for companies to assess the breach and identify its true scope. Instead the NRF believes that a reasonableness standard currently used by many states is the better approach.

Timing for identification of the scope of the data breach will be a key factor as this legislation is pushed through Congress. Obtaining a reasonableness standard rather than a hard deadline, however, seems unlikely given that the proposed legislation is designed to set a national standard.

There were few details in the proposal other than the 30-day time limit. Looking to prior initiatives by the Obama Administration may provide some guidance on where this is going. In the 2011 National Data Breach Initiative, businesses would have 60 days for notification of a breach if there was a risk of harm or fraud, could obtain an extension, and could be exempted under certain circumstances. Penalties proposed in 2011 were up to $1000 a day per consumer and a potential $1 million cap. There was, however, no private cause of action right under this proposal.

The timing on this proposed legislation is unclear, but it should be soon as privacy has become a priority for the Obama Administration and there is bi-partisan support for a national standard. In the short term, this means that all companies with consumer's personal information must continue to follow state law in the event of a breach and will need to update their protocol for identifying and responding to a breach once the legislation is passed. Here's a link to your state law regardless of where the proposed federal legislation comes out, all companies should have an information security plan in place as timing may be short, the process may take you months, and many state statutes provide protection if you follow a plan that is consistent with your state law. We discussed this previously in a prior post, but here it is again.

We will keep you updated as this legislation develops, please call or email if you have any questions on your information security plan or other privacy concerns. Bryant Lamer at blamer@spencerfane or 816.292.8296.

AUTHORS

- Bryant T. Lamer

BLOG TOPICS

- Privacy and Cybersecurity Solutions