Full House To Begin Debate On Data Security and Breach Notification Act After Approval Of Energy and Commerce Committee

By: Jay Shapiro and Michael W. Jervis
Cyber Law and Data Protection Alert
4.16.15

Data security and breach notification responsibilities present significant issues for corporations and their insurers. Currently, businesses must survey the landscape of legislation on a statewide basis when a breach occurs. This week, the House Energy and Commerce Committee approved the Data Security and Breach Notification Act, sending it to the full House for debate. The legislation would set nationwide standards for consumer data protection and mandate procedures for responding to breaches.

Most notably, the bill would create a nationwide rule requiring entities to provide notice of a data breach within 30 days of determining the scope of the breach and securing systems. However, entities would be exempted from the notification requirement if a risk assessment performed in conjunction with the FTC shows there is no reasonable risk of consumers being harmed by the breach. Additionally, federal agencies including the FTC, Secret Service, and FBI would be able to delay notification if doing so is deemed necessary to prevent further breaches or if notification would threaten national security or an investigation. The bill also includes a requirement that the FTC educate small businesses about data security and set up a website in support of that effort.

By setting a nationwide standard, if passed the Act would trump a patchwork of rules which have been imposed by states. At the moment, 47 states have laws setting standards for data breach notification in some form. There have been suggestions that the proposed legislation would actually weaken consumer data security standards with respect to the laws currently in place in some states. For example, the Massachusetts Attorney General's office has taken issue with the Act's preemption of state laws and the FTC Bureau of Consumer Protection Director raised similar concerns at a hearing on the bill. As a result of these concerns, Committee Democrats offered several amendments seeking to make the security standards more specific and to avoid some preemption of state laws. However, these amendments were all defeated. An amendment which caps the federal penalties for some companies passed with Republican support. Ultimately the bill passed on a strict party line vote, with Committee Republicans in support and Democrats opposed.

As nearly all companies now collect and store consumer data of some kind, this bill will be an important one for attorneys and technology professionals to track as it moves on to debate in the full House. If the Act passes it will make compliance with data security regulations more straightforward by offering blanket rules applicable across the country. However, companies will have to evaluate their policies designed to comply with myriad state rules and decide whether to continue complying with the stronger protections currently required by some states but which would be preempted by the new law. Finally, companies will be faced with the prospect of potentially having to coordinate with a wider range of federal agencies, including the FTC, FBI, and Secret Service, when a breach inevitably occurs.

For more information regarding this alert, please contact Jay Shapiro (212.714.3063 ; shapiroj@whiteandwilliams.com) or Michael Jervis (215.864.7042 ; jervism@whiteandwilliams.com).

questions.