

States Continue To Grapple With Data Breach Notification Issues

September 28, 2015

Connecticut's data breach notification law currently requires notification "without unreasonable delay." Effective October 1, 2015, Connecticut will (a) require notice of any breach of security not only "without unreasonable delay," but "not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law"; and (b) require an offer of "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" to each Connecticut resident whose Social Security number was breached or is reasonably believed to have been breached, such services to be provided for a period of not less than 12 months and at no cost to each such resident. Connecticut Attorney General George Jepsen stated that the amended law "sets a floor for the duration of the protection and does not state explicitly what features the free protection must include," and that he may "seek more than one year's protection – and to seek broader kinds of protection – where circumstances warrant." As illustrated in Carlton Fields' data breach notification survey (Expect Focus, Summer 2014), approximately 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring entities to notify individuals of security breaches involving personally identifiable information. Many companies favor federal preemption of state data breach notification laws so they will no longer be faced with the daunting task of complying with so many different notification requirements. However, in a letter to Congress dated July 7, 2015, the National Association of Attorneys General observes there are many federal data breach notification and data security bills pending in Congress, and basically urges that any such federal laws not preempt state laws. The letter, signed by 47 state attorneys general, reasons that federal preemption will leave consumers less protected than they are today, and result in the states' inability to respond to consumer concerns. The letter provides many examples of how states have responded to data breaches, and explains that states need continued flexibility to amend their laws in response to technology and data collection changes.

Related Practices

[Technology](#)

[Cybersecurity and Privacy](#)

[Intellectual Property](#)

Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.