Amendments to the Massachusetts' Data Breach Notification Law Create Additional Notification and Response Requirements

By Colin A. Coleman, John E. Ottaviani, or Brian Reilly

On January 10, 2019, Massachusetts Governor Charlie Baker signed new legislation to amend Massachusetts' data breach notification law. The new law, which will be effective as of April 11, 2019, makes a few changes that are particularly relevant to Massachusetts businesses:

1. Emphasis on Immediate Breach Notification.

Although the new law does not change the requirement that breach notifications be provided as soon as practicable and without unreasonable delay, businesses can no longer wait to provide such notices because the number of affected people has not been ascertained. Instead, businesses will now be required to provide notice as soon as possible, and to supplement the original notice with additional notices as new information becomes available. This may entail sending a series of notices to regulators and affected individuals as the business conducts an ongoing investigation into the breach. Businesses should therefore prioritize providing notice quickly after discovering a breach, even when all relevant information may not yet be known.

2. Enforcement of the Written Information Security Program Requirement.

In addition to other new requirements related to the content and substance of breach notifications, the amendments require breach notices to state whether or not the individual or company maintains a written information security program ("WISP"). WISPs have been required under Massachusetts law since 2010, but many businesses either have not implemented a WISP or have not regularly updated their existing WISPs as required. Going forward, businesses that suffer a data breach without a WISP in place are likely to face extra scrutiny from regulators, which might include enforcement actions by the Attorney General's Office and the imposition of fines and penalties. Any business that does not currently have a WISP in place should make every effort to implement one before the new law becomes effective in April. Businesses that already have WISPs should review and update their current policies to make sure they are in compliance. WISPs are not one-size-fits-all, so businesses should ensure that the program described in their WISP is consistent with the business' actual risks and operating procedures.

3. Mandatory Complimentary Credit Reporting.

If a data breach includes the Social Security numbers of Massachusetts residents, the amendments require the business that suffered the breach to offer affected individuals complimentary credit monitoring for at least 18 months (42 months if the breach involved a consumer reporting agency). Businesses should therefore evaluate their data collection and retention policies to be sure that they only collect and store personal data that is necessary to the operation of its business. In particular, storing consumers' Social Security numbers unnecessarily could result in avoidable costs and administrative burdens associated with providing complimentary credit monitoring following a breach.

If you need help reviewing existing policies or creating new ones, or you would like to discuss ways to help prevent becoming the victim of a cyberattack or scam, please contact Colin A. Coleman, John E. Ottaviani, or Brian Reilly at Partridge Snow & Hahn LLP.

Date Created
January 15, 2019