Client Alert: Massachusetts Expands Breach Notification Requirements

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 1.23.2019

Massachusetts Governor Charlie Baker recently signed House Bill 4806, amending the state's data breach notification law. In relevant part, the amendment expands the information that must be reported to Massachusetts regulators in connection with a data breach involving the personal information of Massachusetts residents, imposes new requirements on compromised entities, and adds some clarification to when entities are required to issue notice of a breach. These changes take effect on April 11, 2019.

Under the amendment, entities that have experienced a data breach involving the personal information of Massachusetts residents are required to inform the Massachusetts Office of the Attorney General and the Office of Consumer Affairs and Business Regulation "whether the person or agency maintains a written information security program" (WISP). Existing Massachusetts law requires "[e]very person that owns or licenses personal information about a resident of the Commonwealth [to] develop, implement, and maintain a comprehensive information security program." 201 CMR § 17.03(1). This new requirement will provide Massachusetts regulators with a mechanism to penalize entities who have failed to implement a compliant WISP.

Additionally, Massachusetts is now the fourth state to require companies to provide free credit monitoring services to affected individuals in data breaches involving Social Security numbers. California and Delaware require at least one year of credit monitoring services when Social Security numbers are compromised, Connecticut requires two years, and Massachusetts now requires eighteen months. Interestingly, in the wake of recent breaches at credit reporting agencies, the amendment requires breached credit reporting agencies to provide 42 months of free credit monitoring services when Social Security numbers are involved. Further, affected individuals cannot be required to waive their right to a private right of action as a condition to receive the credit monitoring services.

The amendment also changes the contents required in breach notifications. For example, companies must now disclose to Massachusetts regulators the types of personal information compromised in the breach. Companies must also inform affected residents that they have the right to place a security freeze on their credit reports at no charge. Additionally, if a subsidiary is breached, the notification to affected residents must now include the name of the parent or affiliated corporations.

Finally, the amendment clarifies that notice cannot be delayed on grounds that the total number of residents affected by the breach is not yet known. Rather, companies must give notice "as soon as practicable and without unreasonable delay" once an entity "knows or has reason to know" of a breach of a resident's personal information.

Companies should update their incident response plans to incorporate these changes and review their written information security policies and procedures for any compliance gaps. For assistance with compliance questions, policy reviews, or incident response preparation, please contact John Landolfi, Christopher Ingram, Sarah Boudouris or your Vorys attorney.