

Massachusetts Imposes Additional Data Breach Notification Requirements

Alysa Z. Hutnik

January 23, 2019

On January 10, 2019, Massachusetts Governor Charlie Baker signed into law the Massachusetts's Data Breach Notification Act, which amends Massachusetts data breach reporting laws. The new law, available [here](#), amends the timing and content of individual and regulator data breach notifications, and provides for credit monitoring services when social security numbers may have been compromised.

Key updates to the state's data breach notification laws include the following:

- **Free Credit Monitoring:** Following breaches involving Social Security numbers, entities must "contract with a third party to provide" free credit monitoring services to impacted Massachusetts residents at no cost for at least 18 months (42 months, if the company is a consumer reporting agency), and provide consumers with instructions on how to access these services.
- **No Mandatory Arbitration Clauses:** Companies are prohibited from asking individuals to waive their right to a private action as a condition for receiving credit monitoring services.
- **Additional Required Information for the Breach Notice:** The required notice to consumers, the Massachusetts Attorney General, and the Office of Consumer Affairs and Business Regulation already provided for under current Massachusetts law must now also include additional information such as the name and address of the person that experienced the breach of security, the person responsible for the breach, if known, and the type of personal information compromised. Entities are also required to submit to regulators a sample of the notification letters that they send to consumers, which will be posted online.
- **Notice Timing:** An entity may not delay notice to affected individuals on the grounds that it has not determined the total number of individuals affected. Rather, the entity must send out additional notices on a rolling basis, as necessary.
- **Disclosure of Parent/Affiliate Company:** If the company experiencing a breach is owned by a separate entity, the individual notice letter must specify "the name of the parent or affiliated corporation."

Under Massachusetts data security regulations (201 CMR § 17.03), any entity that owns or licenses personal information about a Massachusetts resident is currently obligated to develop, implement, and maintain a comprehensive written information security program that incorporates the prescriptive requirements contained in the regulation.

The Massachusetts's Data Breach Notification Act will take effect on April 11, 2019. This is a good opportunity for businesses to update their data breach notification related policies and procedures to ensure that they are in compliance with all state requirements. We will continue to track any updates to state breach notification statutes and post on this blog.