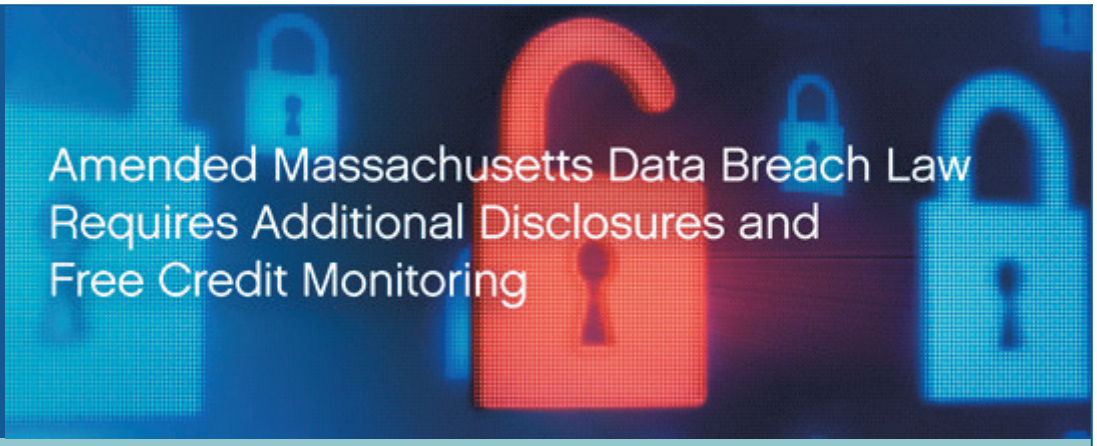
COMMENTARY

JANUARY 2019



Amended Massachusetts Data Breach Law Requires Additional Disclosures and Free Credit Monitoring

IN SHORT

The Situation: In the wake of the Equifax data breach, Massachusetts has amended its data breach law.

The Result: Companies reporting security breaches under the amended data breach law must provide additional information about the incident and their written information security program ("WISP"), and they must provide credit monitoring services to any affected residents whose Social Security numbers were disclosed.

Looking Ahead: Massachusetts's data breach law is now one of the most expansive in the country. The new law also reaffirms the need for companies that own or license personal information of Massachusetts residents to maintain a WISP.

As of April 10, 2019, Massachusetts will implement an amended data breach law, Mass. Gen. L. 93H, initially introduced as a response to the Equifax data breach.

The amendments do not alter the triggers for notification. Rather, they focus on the content of breach notifications and the "mitigation services" companies must offer victims. The most significant amendments: (i) expand the information that companies reporting breaches must disclose; (ii) require companies to provide, at no cost to affected individuals, at least 18 months of credit monitoring services if the breach involved the disclosure of Social Security numbers; (iii) provide that companies shall not delay notice on grounds that the total number of affected Massachusetts residents is unknown; and (iv) increase the public visibility of reported breaches.

Additional Information Required in Breach Notices

The amendments require companies reporting breaches under the law to provide additional information to the Massachusetts Attorney General ("AG") and the Director of the Office of Consumer Affairs and Business Regulation ("OCABR"). Companies typically already provide much of the information now required by law—the company's name and address, the identity of the person reporting the breach and his or her relationship to the entity that experienced the breach—as well as the "the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data."

The law, however, also imposes three new and novel requirements:

- A company must disclose in the notice to the AG and OCABR "the person responsible for the breach of security, if known."
- The amendments require companies to inform regulators whether the company "maintains a written information security program," and whether the company has updated or plans to update the WISP in response to the incident. A WISP has been a legal requirement since 2010 for companies that own or license the personal information of a Massachusetts resident, and must contain appropriate administrative, technical, and physical safeguards for such personal information.
- If the company reporting the breach "is owned by another person or corporation," then the

notice to affected residents "must include the name of the parent or affiliated corporation."

These provisions are unique to Massachusetts's data breach law, and notably expand the regulatory focus from the incident to include the company's information security program.

> The amendments do not alter the triggers for notification. Rather, they focus on the content of breach notifications and the "mitigation services" companies must offer victims.

Mitigation Services for Residents

Massachusetts also joins California, Connecticut, and Delaware in requiring companies to provide identity theft protection or credit monitoring to residents whose Social Security numbers were disclosed in a breach.

The new law requires a company reporting a breach to provide at least 18 months of credit monitoring (consumer reporting agencies must provide at least 42 months), at no cost, to residents whose Social Security numbers were, or are "reasonably believed to have been," disclosed. The company must provide affected residents with all information necessary for enrollment in credit monitoring services, and the company may not require them to waive their right to a private cause of action as a condition to obtaining the services. The company must file a report with the AG and OCABR certifying that its credit monitoring complies with these requirements. The company also must advise residents that consumer credit reporting agencies will not charge them for placing or lifting credit freezes.

Notice Timing

The amendments add a new provision that notice "shall not be delayed on grounds that the total number of residents affected is not yet ascertained." The law contemplates that companies make supplemental notice in these circumstances, providing that "[i]n such case, and where otherwise necessary to update or correct the information required, a [company] shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information."

Increased Public Access to Breach Notifications

The amendments also contain provisions designed to increase the visibility of breaches to the general public, including:

- OCABR will post on its website sample consumer notices received from companies reporting breaches—typically within one business day of receipt; and
- OCABR will instruct consumers on how to file public records requests to obtain copies of the reporting company's breach notification submitted to regulators.

The law contains a number of ambiguities and interpretation questions, which eventually may prompt the OCABR to promulgate further regulations, as permitted under the amendments.

FOUR KEY TAKEAWAYS

1. Companies reporting security breaches under the amended Massachusetts data breach law must disclose more information to regulators and consumers.
2. Notification letters will be more readily available to the public.
3. Companies must provide 18 months of credit monitoring services at no cost to Massachusetts residents whose Social Security numbers are disclosed in a breach.


Lisa M. Ropple
Boston


Daniel J. McLoon
Los Angeles


Mauricio F. Paez
New York


Richard J. Johnson
Dallas

4. Companies that own or license personal information of Massachusetts residents should implement, and where necessary update, a WISP satisfying the Massachusetts legal requirements.

Christopher Hurld, Counsel in the Boston Office, assisted in the preparation of this Commentary.

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

Blockchain Trading for Nonlisted Securities: The New French Regime Is Achieved

FCC Establishes Reassigned Phone Number Database

European Data Protection Board Provides Clarifications on Territorial Scope of GDPR

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide℠