Published on *The National Law Review* https://natlawreview.com

Change in Massachusetts Data Breach Notification Law Highlights Requirement That Organizations Implement a Written Information Security Program (WISP)

Article By:

Michael Waters

Alexander Boyd

Overview

Since 2010, Massachusetts has required organizations that collect personal data about Massachusetts residents to implement a comprehensive written information security program ("WISP") designed to avoid and respond to data security incidents.

Despite this requirement, many companies, particularly those not physically located in Massachusetts, have not done so. Historically, the absence of a WISP is something that went unnoticed, but that may no longer be the case due to a recent change in the Massachusetts breach notification law.

Specifically, Massachusetts has amended its data breach notification law to require organizations that experience a data security incident to notify the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation whether the organization implemented a WISP. This new reporting requirement highlights both the legal and practical need to implement a WISP.

Change in the Law

Effective April 11, 2019, organizations that experience a data breach that exposes the personal information of Massachusetts residents will have new responsibilities under Massachusetts law. In addition to the preexisting requirements that organizations notify the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation regarding the nature of the breach, the number of impacted Massachusetts residents, and the steps taken related to the incident, organizations must now also expressly state whether the organization implemented a WISP. Organizations must also state whether they have updated their WISP after the data incident. While this new requirement does not formally go into effect until April 11, 2019, the Office of Consumer Affairs and Business Regulation has already updated its notification form to ask whether the organization implemented a WISP.

Organizations must also continue to notify impacted Massachusetts residents of the data breach and must now notify the residents that there is no charge to institute a security freeze or credit freeze. If the breach disclosed the Social Security Number of Massachusetts residents, the organization must now provide a minimum of 18 months of credit monitoring services, or 42 months if the organization is a consumer reporting agency. Related to this requirement, the organization may not require Massachusetts residents to waive their right to file a lawsuit in exchange for the credit monitoring services.

What is a Written Information Security Program?

A WISP is designed to develop and document the systems and processes that protect the customer and employee personal information stored by an organization. Under Massachusetts law, a WISP must address certain areas, including:

1) designating employees responsible for the security program;

2) identifying and assessing security risks;

3) developing policies for the storage, access, and transportation of personal information;

4) imposing disciplinary measures for violations of the WISP;

5) limiting access by terminated employees;

6) overseeing the practices of third-party vendors;

7) restricting physical access to records;

8) monitoring and reviewing the scope and effectiveness of the WISP; and

9) documenting steps taken in response to data security incidents.

A WISP must also establish certain computer system security standards when technically feasible, including:

1) securing user credentials;

2) restricting access to personal information on a need-to-know basis;

3) encrypting the transmission and storage of personal information;

4) monitoring of security systems;

5) updating firewalls, security patches, anti-virus, and anti-malware software; and

6) training employees on the proper use of the computer security systems.

The Takeaway

Written information security plans are required for those organizations that collect personal

information from Massachusetts residents and Massachusetts is taking steps to ensure organizations comply with that requirement. Apart from this legal obligation, all organizations should strongly consider implementing and documenting their processes for protecting personal information and for responding to a data security incident. Proactively assessing and addressing information security risks will not only fulfill the organization's requirements under Massachusetts law, but will allow the organization to reduce its risk of a data security incident and be prepared to quickly respond in the event an incident does take place.

National Law Review, Volume IX, Number 103