Plan Now to Comply with New Rhode Island Identity Theft Protection Act

Businesses, organizations, state and local governmental entities and individuals who collect and store personal information about Rhode Island residents should start planning now to comply with the new Rhode Island Identity Theft Protection Act, which goes into effect on June 26, 2016 and replaces the existing law. Businesses and organizations of any size are affected. There are no exemptions due to size.

New obligations imposed include the following:

- Implementing and maintaining a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information, and the purpose for which the information was collected, in order to prevent unauthorized access and to preserve confidentiality of the information
- Retaining personal information no longer than is reasonably required to provide the services requested
- Destroying all personal information in a secure manner (for example, by shredding, pulverizing, incinerating or erasing)

The new law also updates the notification requirements in case of a breach of security. Like the current law, the notice must be given in the “most expedient time possible,” but the new law states that the notice must occur no later than 45 days after confirmation of the breach. However, financial institutions, trust companies and credit unions subject to and examined for and found in compliance with Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice will be deemed in compliance with the new law.

What should businesses and organizations be doing now to comply?

- Assess what types of personal information of Rhode Island residents are being collected, shared or used and who has access to that information. Is there information that does not need to be collected? How is the information being stored? Is the information only being stored as long as needed and being destroyed properly?
- Is the information of Rhode Island residents being shared with third parties (for example, service providers or vendors)? If so, contracts should be reviewed, and amended as needed, to make sure that those who have access to personal information of Rhode Island residents are also subject to written obligations to implement and maintain reasonable security procedures and practices.
- In many cases, the best way to evidence that the business or organization has a risk-based information security program in place is to have a written document detailing the policies and procedures. A business that has adopted a written information security program to comply with the Massachusetts data security requirements is likely to be in compliance with the new Rhode Island law. However, such programs should be reviewed to make sure they cover the personal information of Rhode Island residents.

Complying now will help avoid scenarios such as the following, which have occurred under the similar Massachusetts law:

- A hospital in Rhode Island was fined $150,000 for violating a similar Massachusetts law when it lost 19 unencrypted back-up tapes with patient names and personal information.
- A Rhode Island health insurance company donated a file cabinet without cleaning out protected health information of over 12,000 individuals. No fines were assessed, but the insurance company had to report the breach and offer free credit monitoring to all affected individuals for a year. The company has

since conducted mandatory training for its employees.
- A hospital in Massachusetts was fined $1.5 Million after the theft of a laptop computer containing unencrypted health information of patients and research subjects.

Date Created
February 16, 2016