PUBLICATION

Maryland and Delaware to Roll Out Changes to Data Breach Laws in 2018

Authors: Alisa L. Chestler
August 30, 2017

States continue to amend their Data Protection and Breach Notification Requirements. Maryland and Delaware are the most recent states to pass legislation designed to bring additional precision to an organization's responsibilities with respect to the protection of personal information.

Maryland

Effective January 1, 2018, significant changes to Maryland's Personal Information Protection Act (Md. Code Com Law § 14-3501) will become effective. The amendments alter the standard of when information is considered "breached," the breach of harm analysis and what information is considered "Personal Information." The Act currently requires notification to individuals if an individual's computerized Personal Information is subject to an unauthorized access or acquisition, unless the information was encrypted. The definition of a breach was amended to eliminate access as a criteria, leaving acquisition as the sole standard.

Prior to the amendment, the definition of Personal Information consisted of the individual's first name or first initial associated with the individual's Social Security Account Number, Driver's License Number, a credit or debit card number along with codes that permit access to an individual's financial accounts or the individual's Taxpayer Identification Number. The amendments add to the list of Personal Information: (i) passport or other identification numbers issued by the federal government; (ii) state identification numbers; (iii) Health Information, including information about an individual's mental health; (iv) a health insurance policy or certificate number or a health insurance identification number used by an insurer or a self-insured employer which permits access to an individual's Health Information; (v) biometric data of an individual generated by automatic measurements of the individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image or other unique biological characteristic that can be used to uniquely authenticate the individual's identity when the individual accesses a system or an account; and (vi) a username or email address in combination with a password or security question and answer that permits access to an individual's email account. Health Information is defined as information created by an entity covered by HIPAA, regarding an individual's medical history, medical condition or medical treatment, or diagnosis.

In the event of a breach of Personal Information that is limited to information which allows access to an individual's email account, alternative notice may be provided in electronic or other form that directs the individual to change the password and security questions applicable to the breached account or to take other appropriate steps to protect the account and all other accounts with the same username and email or password or security question or answer.

As amended, an organization that maintains computerized data of an individual residing in Maryland is required to provide breach notification to the individual as soon as practicable, but in no event later than 45 days after the business discovers or is notified of the breach of security of the system containing the individual's Personal Information. The amendment also changes the harm threshold for notice of a Breach to a determination that the unauthorized acquisition of computerized personal information "creates a likelihood that Personal Information has been or will be misused."

Delaware

Delaware's amendments are similar to laws that Massachusetts has enacted. The new Delaware law requires persons conducting business in Delaware and owing, licensing or maintaining personal information on a Delaware resident to "implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." This means that all organizations must document, at a minimum, their basic security understanding and program.

The Delaware amendments are similar to the Maryland amendments in several areas. Delaware has also expanded the definition of "Personal Information" to include many of the same identifiers as Maryland.

Delaware further clarified the instance in which a notification is provided to an individual that their personal information had been subject to a breach. Previously, the Delaware resident was to be notified after an investigation determined that personal information "has been or will be misused." Under the new law, organizations have 60 days to provide notice unless after the investigation the breach of security was determined to be "unlikely to result in harm." Encryption of the personal information remains a safe harbor for information that may have been compromised. The safe harbor is nullified if the encryption key is included as a part of the acquisition and "the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or usable."

The interplay of state data breach notification requirements continues to cause confusion amongst those organizations trying to understand their obligations. Each potential breach requires a fact based analysis that must also take the organization's compliance obligations into consideration along with other laws, insurance requirements and compliance obligations in mind.

If you have any questions regarding the content of this alert, please reach out to Alisa Chestler, CIPP/US or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.