Maryland Amends Personal Information Protection Act

By Joseph J. Lazzarotti

August 8, 2017

Amendments to Maryland's Personal Information Protection Act expand the definition of personal information, modify the definition of breach of the security of the system, provide a 45-day timeframe for notification, allow alternative notice for breaches that enable an individual's email to be accessed, and expand the class of information subject to Maryland's destruction of records laws.

House Bill 974 will become effective January 1, 2018.

Personal Information, Breach of the Security of the System

Maryland's current Personal Information Protection Act, Md. Code Com. Law §14-3501, defines "personal information" as a person's first name or first initial and last name combined with any of the following data elements:

- Social Security number;
- Driver's license number;
- Financial account number, including a credit or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's financial account; or
- Individual taxpayer identification number.

The new amendment expands that definition to include:

- Passport numbers and other identification numbers issued by the federal government;
- State identification card numbers;
- Health information, defined to include any information created by an entity covered by HIPAA regarding an individual's medical history, condition, treatment, or diagnosis;
- A health insurance policy, certificate number, or health insurance subscriber identification number, in combination with a unique identifier that permits access to the information;
- Biometric data, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic that can be used to uniquely authenticate a person's identity upon accessing a system or account; and
- A user name or email address in combination with a password or security question and answer that permits access to the account.

Under current law, a breach of the security of the system includes an unauthorized access or acquisition of computerized personal information. The new law removes "access," leaving breaches limited to unauthorized acquisitions.

Data Breach Investigation, Notification Requirements

A business that owns or licenses computerized data that include personal information of an individual residing in the state that discovers or is notified of a breach of the security of the system must conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of individual has been used or misused as result of a breach. Under the amended law, the individual(s) must be notified if the investigation shows the breach creates a likelihood that personal information has been or will be misused.

The new law also amends the timeframe during which notification must be provided. Notice still must be provided "as soon as reasonable practicable," however, beginning in 2018, notice must not be provided later than *45 days* after the business has concluded its investigation, amending Md. Code Com. Law §14-3504.

The requirement to provide notice of a breach of the security of the system to the Maryland Attorney

Meet the Author

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

General before notifying individuals is unchanged.

The new law permits a substitute form of notice when a breach involves only the loss of personal information that enables access to an individual's email account. Subject to certain exceptions, the business may:

- Provide notice electronically that directs the person to change the password and security questions and answers; and
- Take other steps appropriate to protect the email account with the business and all other online accounts for which the individual uses the same username or email and password or security questions or answers.

This form of substitute notice must be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an internet protocol address or online location from which the business knows the individual customarily accesses the account.

Record Destruction Requirements

Finally, the new law amends Md. Code Com. Law §14-3502 to expand the class of information subject to Maryland's destruction of records laws. The current version law covers only customer records, the amended law covers records relating to employees and former employees that contain personal information.

Data Breach Notification Trends

The country's data breach notification law system consists of a patchwork of state statutes. Currently, 48 states have legislation requiring private or governmental entities to notify individuals of a security breach of information involving their personally identifiable information. In recent years, many states have amended these laws in light of new trends and to keep in line with other states. In 2016 alone, six states amended their breach notification statutes. Businesses should take notice of certain new trends.

Notice requirements incidents involving health or biometric data and username and passwords to online accounts are on the rise. Illinois, Oregon, and Rhode Island have expanded the definition of personal information to require notice when certain forms of health or biometric data are compromised. They now require notice for breaches involving health insurance and medical information. Illinois and Oregon have included biometric information as well, such as retina or fingerprints.

Moreover, California and Florida had been the only two states to require notice when an individual's user name or email address and password were compromised. However, Illinois, Nebraska, Nevada, Rhode Island, and Wyoming have since joined California and Florida in implementing such requirements.

Substitute notice for username and password incidents. Similar to Maryland's new law, Illinois and California allow business entities to provide substitute notice by email to affected individuals with instructions to change their username and password for the affected account and any other associated accounts. Florida and Nevada both require that notice of username or password incidents comply with notice requirements for the data breach of other types of personal information.

***

New trends likely will continue to prompt amendments to state data breach notifications laws. Businesses should develop their incident response plans with flexibility as a key component to ensure compliance with the most current breach notification requirements.

Please contact a Jackson Lewis attorney with questions about this or other legal developments.

*The National Operations Center serves as the firm's central administration hub and houses the firm's Facilities, Finance, Human Resources and Technology departments.