State Data Breach Notification Statutes: 2017 Year in Review

Insights
11.28.17

Continuing a trend in the last few years, in 2017, eight states amended their security breach notification laws to expand definitions of "personal information", specify the timeframe in which notification must be provided, and require businesses to implement adequate security practices to protect personal information in their possession, among other things. New Mexico also enacted a data breach notification statute of its own, leaving only two states without specific legislation relating to data breach notification requirements. A summary of the highlights of the new law and other amendments enacted in 2017 follows:

1. Delaware – The state of Delaware revamped its existing data breach notification statute, including to: (1) expand the definition of "personal information"; (2) mandate offering one year of complimentary credit monitoring services if a breach involves a Delaware resident's Social Security number; (3) require that entities use reasonable diligence to identify and provide notice to Delaware residents that personal information was included in a security breach; (4) provide notification of a breach involving more than 500 Delaware residents to the Delaware Attorney General; and (5) require entities that conduct business within Delaware 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."
2. Illinois – The State of Illinois amended the Personal Information Protection Act to direct that a state agency, that has been subject to or has reason to believe it has been subject to a single breach of the security of data concerning personal information of more than 250 Illinois residents or an instance of aggravated computer tampering, shall notify the Chief Information Security Office and the Attorney General within 72 hours following discovery of the incident.
3. Maryland – The state of Maryland expanded the Maryland Personal Information Protection Act to: (1) expand the definition of "personal information" to include passport/identification numbers issued by the federal government, state identification card numbers, certain health and health insurance policy information, certain biometric data and user name or email address in combination with a password or security question and answer that permits access to the account; (2) include a 45-day timeframe for providing notice of a breach; (3) allow for alternative service when the breach involves only the loss of personal information that enables access to an individual's email account; and (4) expand the information subject to Maryland's destruction of record laws.

4. North Dakota – The state of North Dakota added a section to the North Dakota Century Code relating to "Data breach response and remediation costs", indicating that the Director of the Office of Management and Budget may pay from the Risk Management Fund costs necessary for notification and remediation following a data breach involving a state entity.

5. New Mexico – The state of New Mexico became the 48th state to enact a breach notification statute, requiring that New Mexico residents be notified if their "personal identifying information" was affected by a breach. The statute requires notification to affected individuals within 45 days from the date of discovery of a security breach and notice to the Attorney General and three major credit bureaus if the breach affects more than 1,000 New Mexico residents.

6. Tennessee – The state of Tennessee revised the definitions of "breach" and "personal information" in its data breach law, requiring notification if an unauthorized person acquired either unencrypted data or encrypted data and the corresponding decryption key.

7. Virginia – The Commonwealth of Virginia expanded its breach notification legislation to include income tax information within the types of information that require notification to the Virginia Office of Attorney General. The statute does not, however, require notification to the individual taxpayers regarding a security breach involving income tax information.

8. Washington – The state of Washington enacted a biometric privacy law to address the collection, storage and use and of biometric data (data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual) for commercial purposes. The law requires an entity to disclose how it uses biometric data, and provide certain notices and obtain consent before enrolling or changing the use of an individual's biometric identifiers in a database.

9. Wyoming – The state of Wyoming amended requirements of the State Data Security Plan to ensure the privacy of student data, to impose policies for the collection, access, security and use of student data by school districts and to require school districts to adopt and enforce policies relating to student data.

In addition to the legislation that passed in 2017, some states, such as Illinois and California, amended and/or expanded their data breach notification laws in 2016, and those amendments became effective January 1, 2017. In Illinois, the Illinois Personal Information Protection Act now includes an expanded the definition of "personal information", including medical information, health insurance information, certain biometric data, and user name or email address in combination with a password or security question and answer. The Illinois Personal Information Protection Act also now requires notification to the Illinois Attorney General in certain circumstances where HIPAA-regulated entities are impacted and includes limits to the encryption safe harbor if the encryption key was or is reasonably believed to have been acquired in the data breach.

In California, entities are now required to notify affected individuals of a data breach of encrypted information, if "the encryption key or security credential was, or is reasonably believed to have been,

acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable."

Notably, only two states, Alabama and South Dakota, have not enacted a law requiring notification of a security breach involving personal information.

Related People

Heather Zalar Steele
Partner
610.230.2134
Email