State Data Breach Notification Laws: Overview of the Patchwork

By Joseph J. Lazzarotti, Jason C. Gavejian and Maya Atrakchi

April 9, 2018

The nation's patchwork of state data breach notification laws is now complete. All 50 states, as well as the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, have enacted breach notification laws requiring private organizations or government entities to notify individuals of a security breach involving their personally identifiable information.

The last two states, Alabama and South Dakota, enacted data breach notification statutes in March. The Alabama Data Breach Notification Act goes into effect on May 1, 2018. The South Dakota law will take effect on July 1, 2018.

Additionally, many other states, in response to trends, heightened public awareness, and a string of large-scale data breaches, have continued amending their existing laws. This means data breach notification laws change frequently and keeping up with them can be a challenge.

Requirements Vary

The first state data breach notification law was enacted in 2002 in California. It soon became the model for other states' breach notification laws. In addition, the U.S. Department of Health and Human Services Office of Civil Rights (OCR) adopted a similar structure for covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Common provisions among the breach notification laws include:

- Notification to affected state residents without unreasonable delay;
- Notification to certain agencies including state attorneys general and/or consumer reporting agency under certain circumstances;
- Notification exceptions for good-faith access by an employee, encryption of the data, and determinations of low risk of harm;
- Specific requirements for the content of the notification; and
- Civil penalties enforced by the state's attorney general.

Despite these common threads, abundant variations exist among state law provisions. For example, in some states, notification to state agencies is required only when a certain number of residents of the state are affected by the breach. In other states, notification to state agencies is required regardless of the number of affected residents.

While all states require notification "without unreasonable delay," some states provide a specific timeframe by which notification must be made to affected individuals following discovery of the breach (*e.g.,* within 30, 45, or 60 days).

Further, in some states, only the state's attorney general may institute an action for a violation of the state's law, while other states permit a private cause of action by an affected individual.

Businesses operating in multiple states must be alert to the requirements in the various jurisdictions and the growing trends in recent amendments.

Selected State Provisions

This chart provides a brief summary of some of the key features of state breach notification laws and the states with those features.

Selected Provisions	States/Jurisdictions

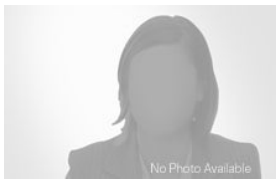
Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email



Maya Atrakchi

KM Attorney
New York Metro
New York City 212-545-4000
Email

Practices

Privacy, Data and Cybersecurity

Industries

Automotive
Chemicals
Construction
Energy and Utilities
Financial Services
Government Contractors
Healthcare
Higher Education
Hospitality
Insurance
Life Sciences
Manufacturing

Selected Provisions	States/Jurisdictions
Expanded definition of personal information	Alabama, Alaska, California, Connecticut, Delaware, Florida, Georgia, Illinois, Iowa, Kansas, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, Wisconsin, Wyoming, District of Columbia, and Puerto Rico.
Content requirements for notifications	Alabama, California, Florida, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, Montana, New Hampshire, New Mexico, New York, North Carolina, Oregon, Rhode Island, South Carolina, Vermont, Virginia, Washington, West Virginia, Wyoming, and Puerto Rico.
Notification to state agency required (requirements in some states may depend on minimum number of residents affected by the breach)	Alabama, Alaska, California, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, Washington, Wisconsin, and Puerto Rico.
Credit monitoring required	California, Connecticut, and Delaware.
Risk of harm	Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

Trends in State Statutory Amendments

Expanded definition of personal information

Generally, the notification obligations of state data breach statutes are triggered when a "breach of security" affects "personal information," as defined in the statute.

Personal information commonly is defined as an individual's first name or first initial and last name in combination with an additional data element, such as a Social Security number, driver's license number, or financial account information with the applicable PIN or access code for same. Recently, however, many states have amended their statute's definition of "personal information" to include additional data elements, such as biometric and health information and user name or email address and password.

For example, Illinois, Oregon, and Rhode Island have expanded their definition of personal information to require notice when certain forms of health insurance, medical, and/or biometric (*e.g.,* retina and fingerprints) data are compromised. The newly enacted South Dakota law also includes both health and

biometric data in its definition of personal information. New Mexico's new law includes biometric data. The new Alabama law also includes certain kinds of health information.

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. Now, Alabama, Illinois, Nebraska, Nevada, Rhode Island, South Dakota, and Wyoming have joined them in adopting such requirements.

Implementation of reasonable security measures

Designed to prevent data breaches in the first place, and likely to become more prevalent due to concerns over recent large-scale data breaches, at least 15 states have some form of a generally applicable "reasonable safeguards" requirement. This is a requirement that organizations implement reasonable security measures to enhance protection of personal information from unauthorized access, acquisition, use, or disclosure. Such obligations require significant efforts, reaching most, if not all, parts of an organization, remaking data breach response measures into preventive measures.

Massachusetts regulations, considered the benchmark for state data security obligations, go further than a general requirement to have reasonable safeguards. The regulations set out specific safeguards in order for organizations to be in compliance. These include maintaining a written information security program, conducting a risk assessments, ensuring third-party service providers are safeguarding personal information, and encrypting personal information on portable data storage devices. New York and North Carolina are considering updates to their respective laws that would impose similar data security requirements as Massachusetts'.

California law, on the other hand, includes a more general requirement that entities that own or license personal information about California residents implement and maintain reasonable security measures and procedures to protect that information. The recently enacted New Mexico and Alabama laws include similar provisions, and Illinois had amended its law to include such a provision as well. Other states with reasonable-security-measure requirements include: Arkansas, Delaware, Florida, Nevada, Indiana, Maryland, Connecticut, New Jersey, Oregon, Rhode Island, and Utah.

In February 2016, California's then-Attorney General Kamala Harris issued the California Data Breach Report, which analyzed the data breaches reported to her office from 2012–2015. Perhaps the most consequential part of the Report for businesses is that it established a floor of controls (*i.e.,* compliance with the Center for Internet Security's Critical Security Controls). A business must implement these controls to be considered to have adopted "reasonable safeguards" to protect personal information.

Takeaways

Today's nationwide patchwork of state breach notification laws require data holders operating in multiple states or maintaining personal information of residents of multiple states to keep up with the requirements across many jurisdictions.

Organizations should consider the following to help them meet the requirements by establishing good baseline policies and practices:

- Develop a written information security program;
- Train employees on data security;
- Conduct regular data security assessments;
- Run tabletop security exercises; and
- Prepare breach notices templates in advance of any breach.

Please contact your Jackson Lewis attorney to discuss these developments and specific state breach notification laws and reasonable safeguard requirements.

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