JULY 2015

COMMENTARY

# States Aggressively Amend Data Breach Notification Obligations

In his State of the Union Address earlier this year, President Obama emphasized an urgent need for comprehensive cybersecurity and privacy legislation. The President's statement capped a week-long promotional effort in support of various White House privacy and cybersecurity initiatives, perhaps most notably including the creation of a national data breach notification standard. Citing the cost and confusion caused by 47 different state data breach notification statutes, the President proposed the Personal Data Notification and Protection Act, which would preempt state notification statutes and establish a 30-day notification requirement from the discovery of a data breach. In the face of various political impediments, however—namely, concerns over preemption and/or weakening of existing state standards—a national data breach notification scheme has proven an elusive goal.

## Where Congress is Thwarted, State Legislatures May Be Encouraged

As noted by the President, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach notification laws that generally require, with certain exceptions, that individuals affected by data breaches be notified of the breach. Kentucky is the latest state to do so. Alabama, New Mexico, and South Dakota are the lone holdouts. These laws generally identify the entities required to provide notification to others of a data breach, those who should receive such notification, the circumstances that trigger notification obligations, the types of personal information to which the laws pertain, and exceptions to and/or exemptions from notification obligations. The laws differ from state to state, however, and are amended with increasing regularity.

As set forth in the table below, a number of notable amendments to state data breach notification laws have recently taken effect, or may do so soon. From the amendments, clear trends emerge:

- Illinois, Montana, Nevada, North Dakota, Oregon, Rhode Island, and Wyoming have expanded the definition of "personal information" to protect a greater number of data types, such as medical and insurance information, biometric data, and email addresses.
- Illinois and Rhode Island, like Massachusetts and others before them, have enacted or may enact data protection laws as a complement to existing data breach notification laws.
- Illinois, Montana, North Dakota, Oregon, Rhode Island, and Washington have joined or may join a

large list of states that require that state attorneys general and/or other government bodies be notified of data breaches.

- Connecticut, Rhode Island, and Washington require that individuals be notified of data breaches within an express deadline, either 45 or 90 days from "confirmation" or "discovery" of a breach.

These states are the most recent to amend their existing data protection and breach notification laws. But they will not be the last. Companies should monitor future data breach legislation and remain mindful of their incident readiness and response programs, which should be reviewed regularly to ensure compliance with this evolving legislative framework.

One thing is certain: The previously noted trends signal greater government scrutiny of corporate cybersecurity practices, not less.

| State | Amendment's Effective Date | General Description of Certain Key Provisions |
|---|---|---|
| Connecticut<br>(S.B. No. 949) | October 1, 2015 | Requires data breach notification to individuals not later than 90 days after discovery of a breach, unless less time is required under federal law.<br><br>Requires the provision of appropriate identity theft prevention services and, if applicable, identity theft mitigation services, at no cost to the consumer for a period of not less than 12 months. |
| Illinois<br>(S.B. No. 1833) | If signed by the Governor, it would become effective on June 1, 2016<br><br>The amendment was sent to the Governor for signature on June 29, 2015. It passed Senate on April 22, 2015, and House on May 28, 2015 | Expands the definition of "personal information" to include a name in combination with health insurance information, medical information, unique biometric data, geolocation information, and consumer marketing information.<br><br>Expands the definition of "personal information" to also include user name or email address, in combination with a password or a security question and answer.<br><br>Requires notification to the Attorney General of data breaches involving more than 250 Illinois residents, within 30 business days from the discovery of the breach or when notice to consumers is provided, whichever comes sooner.<br><br>Includes data security provisions that require data collectors to maintain reasonable security measures to protect data from unauthorized access and to maintain similar contractual provisions.<br><br>Requires certain entities to post a privacy policy. |
| Montana<br>(H.B. No. 74) | October 1, 2015 | Expands the definition of "personal information" to include a name in combination with medical record information or a taxpayer identification number.<br><br>Requires notification to the Attorney General's consumer protection office. |

| State | Amendment's Effective Date | General Description of Certain Key Provisions |
|---|---|---|
| Nevada<br>(A.B. No. 179) | July 1, 2015, but not applicable to data collectors or a business until July 1, 2016 | Expands the definition of "personal information" to include a name in combination with medical information or a health insurance number.<br><br>Expands the definition of "personal information" to include a name in combination with a user name, unique identifier, or email address, along with a password, access code, or security question and answer. |
| North Dakota<br>(S.B. No. 2214) | August 1, 2015 | Expands the definition of "personal information" to include a name in combination with an identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password.<br><br>Requires notification to the Attorney General of data breaches involving more than 250 North Dakota residents. |
| Oregon<br>(S.B. No. 601) | January 1, 2016 | Expands the definition of "personal information" to include a name in combination with data from automatic measurements of a consumer's physical characteristics, a consumer's health insurance policy or subscriber identification number in combination with any unique identifier that the insurance provider uses to identify the consumer, or any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.<br><br>Requires notification to the Attorney General of data breaches involving more than 250 Oregon residents. |
| Rhode Island<br>(S.B. No. 134) | June 26, 2016 | Expands the definition of "personal information" to include a name in combination with medical or health information, and email addresses with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.<br><br>Requires data breach notification to individuals not later than 45 days after confirmation of a breach.<br><br>Requires notification to the Attorney General and major credit reporting agencies of data breaches involving more than 500 Rhode Island residents.<br><br>Broadens notification obligations to include breaches involving personal information in paper as well as electronic form.<br><br>Includes data security provisions that require any person who stores, collects, processes, maintains, acquires, uses, owns, or licenses personal information to implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate in view of the size and scope of the organization, and the nature of the information and purpose for which the information is collected, and to maintain similar contractual provisions.<br><br>Precludes data retention for a period longer than is reasonably required to meet the purpose for which the data was collected, or in accordance with a written retention policy.<br><br>Defines "encrypted" to require the use of a 128-bit algorithmic process.<br><br>Increases the penalties for knowing and willful violations to $200 per record and eliminates the $25,000 penalty limit. |

| State | Amendment's Effective Date | General Description of Certain Key Provisions |
|---|---|---|
| Washington<br>(H.B. No. 1078) | July 24, 2015 | Broadens notification obligations to include breaches involving non-computerized personal information.<br><br>Requires data breach notification to individuals not later than 45 days after the breach was discovered.<br><br>Requires notification to the Attorney General and major credit reporting agencies of data breaches involving more than 500 Washington residents not later than 45 days after the breach was discovered.<br><br>Provides that notification is not required if any breach is not reasonably likely to subject consumers to a risk of harm.<br><br>Covered entities and financial institutions are deemed compliant provided they comply with HIPAA and GLBA, respectively. |
| Wyoming<br>(S.F. No. 35)<br>(S.F. No. 36) | July 1, 2015 | Requires notice be "clear and conspicuous" and include, at a minimum, the types of personal identifying information reasonably believed affected, a general description of the incident, the approximate date of the breach, the general actions taken by the company to prevent further breaches, advice directing affected persons to remain vigilant by reviewing account statements and credit monitoring reports, and whether notification was delayed as a result of law enforcement investigation.<br><br>Expands the definition of "personal information" to include account number, credit card number, or debit card number in combination with any security code, access code or password, federal or state government-issued identification card, shared secrets or security tokens known for use in data-based authentication, a username, or email address in combination with a password or security question and answer, a birth or marriage certificate, medical and health insurance information, unique biometric data, and an individual taxpayer identification number. |

## Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.


**Daniel J. McLoon**
Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

**Jay Johnson**
Dallas
+1.214.969.3788
jjohnson@jonesday.com

**Mauricio F. Paez**
New York
+1.212.326.7889
mfpaez@jonesday.com

**Nicole M. Perry**
Houston
+1.832.239.3791
nmperry@jonesday.com