BAHRA

Boulder Area Human Resource Association

jacksonlewis.

State Data Breach Notification Laws: Overview of the Patchwork

"Legal Minute" -- April 19, 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 agency under certain circumstances;
- Notification exceptions for good-faith access by an employee, encryptio 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[1]

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**
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.

[1] Attached is a summary of the Colorado statute.

Selected Provisions	States/Jurisdictions
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.

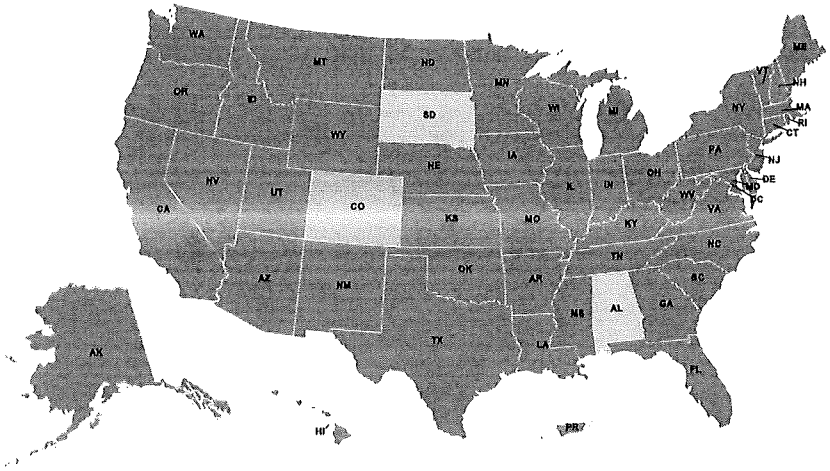
Please contact BAHRA, your attorney, or Pete Bulmer (BulmerP@jacksonlewis.com) to discuss these developments and specific state breach notification laws and reasonable safeguard requirements.

Data Breach Laws Print

Search Criteria

State

Colorado



Records 1 to 1 of 1

?

No Title

What is a breach?

A breach of the "security of the system" is defined as the unauthorized acquisition of unencrypted computerized data that comprises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

Exception: Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or breach is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.

Who is subject to the law?

Covered entities: The law applies to an individual or a commercial entity that conducts business in Colorado that owns or licenses computerized data that includes personal information about a resident of Colorado.

Service provider requirement: An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Colorado resident occurred or is likely to occur

What kind of personal information, if breached, would require notification?

Personal information means an individual's first name or initial and last name in combination with any one or more of the following data elements;

- Social security number;
- driver's license number or identification card number;
- account number, credit or debit card number, in combination with any required security coded, access code, or password that would permit access to an individual's financial account.

How soon must notice be provided to individuals affected by the breach?

Notice must be made in the most expedient time possible and without unreasonable delay, taking into account the legitimate needs of law enforcement, and any measures necessary to determine the nature and scope of the breach and to restore reasonable integrity to the company's information systems.

Who must be notified?

Colorado residents who are affected by the breach must be notified.

In addition, if an individual or commercial entity is required to notify more than 1,000 individuals of a breach of the security of the system, the individual or commercial entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified.

What must the notice say?

Colorado currently has no specific content requirements for the notification letters.

How can notice be provided?

Notice may be provided as follows:

- Written notice to the postal address listed in the records of the person or commercial entity;
- Telephonic notice;
- Electronic notice, if primary means of communication by the person or commercial entity with an individual is by electronic means or if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act; or
- Substitute notice, if the individual or the commercial entity required to provided notice demonstrates that the cost of providing notice will exceed $250,000, that the affected class of individuals to be notified exceeds 250,000, or that the individual or commercial entity does not have sufficient contact information to provide notice.

Is notification required if the information was encrypted?

No, unless there has been a disclosure of unencrypted computerized data, notice is not required.

?

Is notification to a state agency required?

Notification to a state agency is not required.

However below is the contact information for the Attorney General:

Colorado Attorney General Website: **https://coag.gov/**

Mailing: Colorado Department of Law

Ralph L. Carr Judicial Building

1300 Broadway, 10th Floor

Denver, CO

Telephone: 720-508-6000

Fax: 720-508-6030

What are the penalties for not complying with a notification requirement?

The Colorado Attorney General may bring an action in law or equity to address direct violations to the data breach law, to ensure compliance and/or recover direct economic damages from the violation.

A private right of action is not available.

Is notification required to a credit-reporting agency?

If notification of more than 1000 affected Colorado residents is required, all consumer credit reporting agencies that compile files on individuals on a nationwide basis must be notified without unreasonable delay of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified.

Contact information for Credit-Reporting Agencies:

Equifax Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
Email: **security.dataadministration@equifax.com**
Phone number: 1-866-510-4211
Website: **http://www.equifax.com/help/data-breach-solutions/**

Experian
Experian- CRG
P.O. Box 2390
Allen, TX 75013
Email: **databreachinfo@experian.com**
Website: **http://www.experian.com/data-breach/data-breach-information.html**
Phone number: 1 866 751 1323

Transunion
P.O. Box 1000
Chester, PA 19022
Online submission form for reporting a data breach: **https://tudatabreach.tnwreports.com/**
Additional information: **https://www.transunion.com/resources/transunion/doc/solutions/resources/solution-data-breach-services-proactive-br.pdf**

Is a risk of harm analysis available in determining when notification is triggered?

After a reasonable investigation, a commercial entity must give notice of a breach unless the investigation determines that the misuse of information about a Colorado resident has not occurred or is not reasonably likely to occur.

Is credit monitoring required?

Credit monitoring is not required.

Instructions/Commentary/Examples

Instructions

- ***Protecting Personal Information: A Guide for Business***, *available at*, **http://www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personal-information-guide-business_0.pdf**
- ***How to Protect Your Customers***, *available at* http://www.stopfraudcolorado.gov/fraud-center/identity-theft/how-protect-your-customers

?