Published on *The National Law Review* https://natlawreview.com

Update on State Breach Notification Laws: Wyoming, Montana and Alabama

Article By:

Amy C. Pimentel

In the first few months of 2015, a number of states have introduced data breach notification bills and proposed legislative amendments designed to enhance consumer protection in response to increasingly high profile data breaches reported in the media. This activity at the state level seems to indicate that protecting consumers from data breaches is one area where democrats and republicans can find common ground.

From the text of these bills, some of which have already become law, we see two emerging trends: (1) an expansion of the definition of personal information to include more categories of data that, if compromised, would trigger a notification requirement, and (2) the addition of a requirement to notify state agencies (such as attorneys general and state insurance commissioners) where none previously existed.

Here are developments in three states reflecting these emerging trends:

Wyoming

In late February, Wyoming passed two bills that amend its existing data breach notification law by specifying the content required in notices to Wyoming residents, modifying the definition of personal information, and providing for covered entities or business associates that comply with HIPAA to be deemed in compliance with the state individual notice requirements.

In particular, Wyoming's definition of personal information will now include the following:

- Shared secrets or security tokens that are known to be used for data-based authentication;
- A username or email address, in combination with a password or security question and answer that would permit access to an online account;
- A birth or marriage certificate;

- Medical information (a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional);
- Health insurance information (a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history);
- Unique biometric data (data generated from measurements or analysis of human body characteristics for authentication purposes); and
- An individual taxpayer identification number.

These changes to Wyoming law will become effective July 1, 2015.

Montana

Beginning October 1, 2015, amendments to Montana's breach notification law will require entities that experience a data breach affecting Montana residents to notify the Montana Attorney General and, if applicable, the Commissioner of Insurance. Notification must include an electronic copy of the notice to affected individuals, a statement providing the date and method of distribution of the notification, and an indication of the number of individuals in the state impacted by the breach. Entities must provide notice to state regulators simultaneously with consumer notices.

The recent amendments to the Montana law also expand the definition of personal information to include medical record information, taxpayer identification numbers and any "identity protection personal identification number" issued by the IRS. The law specifies that medical information is that which relates to an individual's physical or mental condition, medical history, medical claims history or medical treatment, and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

Alabama

Alabama is one of three U.S. states (New Mexico and South Dakota are the other two) that have not yet enacted a data breach notification law. This may change, however, if Senate Bill 206, the Alabama Information Protection Act of 2015, gains momentum in the state legislature.

The bill would create an obligation to notify individuals and the Alabama Attorney General (for breaches affecting more than 500 individuals) within 30 days of discovering a breach of personal information, and all consumer reporting agencies (for breaches affected more than 1,000 individuals) of the timing, distribution and content of the notices.

Under the Alabama Information Protection Act, personal information will include a person's first name or first initial and last name in combination with any of the following data elements:

- A social security number;
- A number issued on a government document used to verify identity (such as a driver's license, identification card number, passport number or military identification number);
- A financial account number or credit/debit card number, in combination with any required security code, access code or password necessary to permit access to an individual's financial account;
- Any information regarding an individual's medical history, physical or mental condition, or medical treatment or diagnosis by a health care professional; and
- An individual's health insurance policy number, subscriber identification number or any

unique identifier used by a health insurer to identify an individual.

Like California and Florida's new requirements, the proposed definition of personal information would also include a username or e-mail address in combination with a password or security question and answer that would permit access to an online account.

Importantly, entities that are providers of health care, a health care service plan, a health insurer or a covered entity governed by the HIPAA Security and Privacy Rules will be deemed to be in compliance with the law. The Act will not apply to financial institutions subject to and in compliance with the Gramm-Leach-Bliley Act.

Key Takeaways for Businesses

What this means for businesses is that incident response planning is key. Organizations need to have an incident response plan that considers who must be notified, when they must be notified and what these required notices must contain. In addition, organizations need to keep in mind that as we continue to increase the scope of what is considered "personal information," so will we increase the frequency that a particular security incident might trigger notification requirements.

National Law Review, Volume V, Number 127