50 out of 50: Every state in US now has a breach notification law

Colin M. Battersby, Dominic A. Paluzzi, James J. Giszczak | Friday, April 6, 2018

The day has finally come. Every state in the U.S. now has a breach notification law, despite constant pressure for one uniform national law. Alabama and South Dakota have joined the 48 other states and the District of Columbia in enacting data breach notification statutes days apart, with South Dakota's statute enacted on March 21, 2018, and Alabama's statute enacted on March 28, 2018.

Alabama

In a perfect example of the expression "last but not least," Alabama's statute goes beyond post-data breach notification requirements to impose affirmative information security obligations on entities. Specifically, Alabama, as of the effective date of June 1, 2018, requires the implementation and maintenance of reasonable security measures to protect personally identifiable information (PII) against a breach of security, joining a growing but still relatively small list of states with such obligations.

Like the breach notice laws in most states, the new statute requires covered entities to notify individuals affected by such breaches if the covered entity concludes that sensitive PII has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to that individual. But in another example of going beyond the norm, Alabama provides a more expansive definition of PII than is seen in some other states. While PII in Alabama includes the traditional categories of a person's full name or first initial and last name in combination with a social security number, drivers license number or financial account number with other information making

account access possible, it also expressly includes:

- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain PII

Other noteworthy elements of Alabama's new law include a requirement that notice to affected individuals be provided within 45 days after determination that a breach has occurred or upon receiving notice from a third-party, and the possibility of a $5,000 penalty per day for each consecutive day that an entity fails to reasonably comply with the statute. The statute also applies directly to third party agents of covered entities and requires them to notify covered entities of breaches within 10 days of the breach or having come to the reasonable belief that the breach occurred, among other obligations.

South Dakota

South Dakota's new statute does not come with proactive information security obligations, but it is robust in its own right. First, it requires notification to South Dakota residents whose personal or protected information has been or is reasonably believed to have been acquired by an unauthorized person within 60 days unless a delay is necessary for law enforcement purposes. Additionally, it applies to breaches affecting the traditional categories of information described above, as well as:

- Health information as defined under HIPAA.
- An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.
- A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account

Like Alabama, South Dakota's new law includes strong financial incentive for compliance, providing for the possibility of fines of up to $10,000 per day per violation for non-compliance.

It is time to update your incident response plans to reflect these new laws!

For questions regarding data privacy or cybersecurity, including obligations to give notice of a data breach in compliance with state and federal laws, please contact one of the McDonald Hopkins attorneys listed below.

Colin M. Battersby

Dominic A. Paluzzi

50 out of 50: Every state in US now has a breach notification law

James J. Giszczak