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

State Data Breach Notification Laws – Overview of Requirements for Responding to a Data Breach – Updated October 2018

Article By:

Sheila A. Millar

Tracy P. Marshall

With the ever-changing complexity of state data breach notification laws, companies facing a data breach need resources that will help them understand the issues. This summary provides an overview of the similarities and differences in data breach laws adopted in the 50 United States and the District of Columbia. Alabama and South Dakota became the last states to adopt breach notification laws, which took effect on May 1, 2018 and July 1, 2018, respectively. Since our last update, the Colorado law was amended by requiring notice to affected residents and the state's Attorney's General within 30 days of the determination of a breach, imposing content requirements for notices to residents, and expanding the definition of "personal information." As a practical matter, most companies that experience a breach will be required to comply with all or several state laws depending on where the data subjects reside, and international data breach notification laws may also apply.

Because privacy is a politically popular topic for legislators, laws continue to evolve and change. It is important to confirm that no changes have been made to relevant laws whenever you experience a data breach. While this summary focuses on data breach notification obligations, many state laws also impose specific data security requirements for companies that handle personal information, which should also be consulted.

This summary is intended to provide general information about applicable laws, and does not constitute legal advice regarding specific facts or circumstances.

Click here to view.

National Law Review, Volume VIII, Number 277