D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

MARCH 2018

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>> ALERT

SOUTH DAKOTA BECOMES 49TH STATE TO PASS DATA BREACH NOTIFICATION LAW

Once it becomes law, a bill passed unanimously by the South Dakota legislature will make South Dakota the 49th state with a data breach notification law. (Alabama, the only state left without a data breach notification law, is working on passing its own law). South Dakota's new bill comes with the enforcement date looming ahead for the European Union's (EU's) General Data Protection Regulation (GDPR), which for the first time introduces a broad security breach notification obligation in the EU. Therefore, now is the time for companies to review and update their incident response programs.

Key provisions of South Dakota's Senate Bill 62 follow similar trends seen in other recent state data breach notification legislation. For example, the South Dakota bill provides a more expansive definition of personal information, and would make the state one of the many states requiring companies to provide notice of a breach within a specific number of days. In this case, the South Dakota bill requires notification to consumers within 60 days from the time a company learns of the breach. In addition, the bill allows the attorney general to recover up to $10,000 per day per violation, as well as attorney's fees and costs.

NOTIFICATION AND DISCLOSURE REQUIREMENTS

At the core of the bill is an obligation on the information holder to disclose a breach to "any resident" of South Dakota whose personal or protected information was, or reasonably was believed to have been, acquired by an unauthorized person. Notification is not required, however, if after an investigation and notice to the attorney general, the company "reasonably determines that the breach will not likely result in harm" to an affected person.

As noted above, the disclosure must occur within 60 days from the discovery or notification of the breach of system security, but permits a delay in notification in certain instances to avoid impeding a criminal investigation. Other state laws have notification deadlines ranging from 30 to 90 days.

Senate Bill 62 also requires notification to all consumer reporting agencies and any credit bureaus that compile and maintain files on consumers on a nationwide basis, as well as to the attorney general in cases where more than 250 consumers are affected.

THE BOTTOM LINE

A patchwork of state, federal and international rules impose data breach notification obligations on companies. Every company subject to these rules must have a data breach response plan in place that complies with each state's requirements.

"PERSONAL INFORMATION" UNDER THE BILL

The information that is subject to the data breach law is broader in scope than many other states; however, this is consistent with recent data breach notification legislation. More specifically, the data breach law defines "personal information" as a person's first name or first initial and last name, in combination with other data, such as:

- a Social Security or driver license number or other unique identification number created or issued by a governing body;
- health information, as defined under the Health Insurance Portability and Accountability Act (HIPAA);

>> continues on next page

- an employment identification number in combination with any required security code, access code or password, as well as biometric data generated from measurements or analysis of human body characteristics used for authentication;
- an account, credit card or debit card number in combination with any required security code, access code, password, routing number, PIN or any additional information that would permit access to a person's financial account; or
- a username or email address, in combination with a password, security question answer or other information that permits access to an online account.

A unique difference in the South Dakota law compared to many other state data breach notification laws is that, while all of the above bullet points when combined with a person's first name or first initial and last name trigger an obligation to notify customers about a breach, the last two bullet points, even when breached individually (and regardless of whether they are combined with the person's name) also trigger the notification obligation under a "protected information" provision in the law. Most state laws do not include an additional "protected information" definition.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Justin H. Lee
Associate
212.468.4894
jlee@dglaw.com

Vivian Wang
Associate
212.468.4927
vwang@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com