Breach Notification Hits the Big 5-0: Now the Law in All U.S. States

April 24, 2018

With the adoption of breach notification laws in Alabama and South Dakota, all 50 states now have these laws. Companies dealing with multistate breaches can no longer leave any state out of their response plans. Recent amendments to the Iowa and Arizona laws also add to the obligations of responding companies.

THE NEW SOUTH DAKOTA AND ALABAMA LAWS

South Dakota became the 49th state to enact a breach notification statute on March 21, 2018. The statute becomes effective July 1, 2018. Alabama's new law was signed on March 28, 2018 and goes into effect on May 1, 2018. Breach notification is now the law in all 50 states, as well as the District of Columbia, the U.S. Virgin Islands, and Puerto Rico.

Debevoise & Plimpton

The South Dakota and Alabama laws largely track those of other states. Both mandate disclosure to affected state residents. Disclosure to the state attorney general is required too—in South Dakota, when more than 250 residents are affected, and in Alabama, when the number tops 1,000. Like many other states, both South Dakota and Alabama exempt entities that have, and discharge, breach notification obligations under federal law.

These new statutes do go beyond most of their brethren in a few important ways. For one thing, both have teeth. South Dakota allows for fines of up to $10,000 per day per violation. Alabama allows for fines up to $5,000 per day, as well as fines up to $500,000 for knowing violations. There can be actions for damages, too. Alabama's statute applies not just to data owners but also to their third-party agents, who are required to notify their principals if the agent experiences a breach. Alabama also joins the growing body of states that require disclosure, but also impose substantive security requirements: in this case, the "[a]doption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards."

THE IOWA AND ARIZONA AMENDMENTS

Iowa enacted an update to its breach notification statute on April 10, 2018. Iowa has long had the typical provision allowing a breached company not to disclose if the data

exposed by the breach was encrypted. Iowa has now added "pursuant to accepted industry standards" to its definition of encryption. It becomes the ninth state (including California) to mandate some form of encryption standards as a condition for relying on the encryption exception to disclosure.

On April 11, 2018, Arizona updated its breach notification law to expand the definition of personal information that, if breached, triggers mandatory notifications. The definition now includes:

- A first name (or initial) and last name, in combination with any of these:
  - Private keys used to authenticate or sign an electronic record or biometric data used to access an online account (e.g., fingerprint or face scan).
  - Information about an individual's medical or mental health.
  - Together with additional personal information: Social Security, driver's license, financial account, credit or debit, health insurance identification, passport, or taxpayer identification number.
- A username or email address in combination with a password or security question and answer.

Arizona joins states like California, Florida, and Illinois that now include usernames and passwords in their definitions of personal information.

HOW TO RESPOND

These changes are a reminder that breach notification law is not static, so incident response plans cannot be either. Companies holding data of residents in Alabama, Arizona, Iowa, or South Dakota should consider reviewing their cybersecurity programs to ensure compliance. This is also a good moment to recall that breach notification becomes a legal mandate across the European Union on May 25, when the General Data Protection Regulation takes effect. Once a patchwork quilt with holes here and there, breach notification requirements now fully blanket the U.S. and Europe.

These changes are also a reminder that cybersecurity is best seen as an ongoing partnership between a company's legal team and its information security team. How can a company know whether it meets Iowa's new legal test of "accepted industry standards" for encryption, or Alabama's new requirement of "appropriate information safeguards"? The answer is through teamwork between Legal and InfoSec.

* * *

We would be pleased to discuss these issues with our clients and friends.

New York

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

Julia Shu
lshu@debevoise.com

Maxwell K. Weiss
mkweiss@debevoise.com

Washington, D.C.

Luke Dembosky
ldembosky@debevoise.com