Colorado Enacts New Data Security Law – Are You in Compliance?

Insights
6.18.18

On May 29, 2018 Governor Hickenlooper signed HB—1128 into law. Importantly, the Bill amends the State's data breach notification law to require that affected Colorado residents be notified within 30 days of a data breach, and specifies the information that must be included in the data breach notice. The new law, which takes effect September 1, 2018, applies to "covered entities," (if your business maintains, owns, or licenses information of Colorado residents, regardless of where the business or data is based, it is a "covered entity"), also sets forth certain data security requirements, and adds requirements regarding the disposal of personal identifying information.

Among other amendments to Colorado's existing data breach notification law, the new law defines "personal information" as a combination of a Colorado resident's first name or initial and last name along with one or more of the following: (1) Social Security number; (2) student, military or passport identification number; (3) driver's license number or identification card number; (4) medical information; (5) health insurance identification number; or (6) biometric data. The definition of "personal information" also includes a Colorado resident's (1) username or email address in combination with a password or security questions and answers that would enable access to an online account and (2) account number or credit or debit card number in combination with any required security code, access code or password that would enable access to that account.

Colorado residents affected by the breach must be notified of the breach within thirty (30) days (with no extensions!), and the Colorado Attorney General must also be provided notice of the breach if over 500 residents are affected, or reasonably believed to have been affected, regardless of what other security breach procedures the entity might maintain.

The notice must contain certain information, including (1) the date or estimated date or estimated date range of the breach; (2) a description of the personal information breached or reasonably believed to have been breached; (3) the entity's contact information; (4) the toll-free numbers, addresses and websites for consumer reporting agencies and the FTC; and (5) a statement that the Colorado resident can obtain information from the FTC and the credit reporting agencies regarding fraud alerts and security freezes. If the breach involves a Colorado resident's username or email address in combination with a password or security questions and answers that would enable access to an online account, the entity must also direct affected individuals to take appropriate steps to protect their online accounts.

Additional provisions of the bill require covered entities to ensure that third-party vendors protect person information before it is shared with the vendor and to implement written policies governing secure document disposal.

The new law does not include exemptions for size or type of entity, and coverage extends to government agencies. The law authorizes the Attorney General to bring an action to ensure compliance and/or recover damages, and authorized relief may include criminal charges.

Related People

Danielle S. Urban, CIPP/E
Partner
303.218.3650
Email