Tracy Gray

Partner
303.473.2703
Boulder
tbgray@hollandhart.com

Mark Langer

Associate
303.295.8552
Denver
mdlanger@hollandhart.com

Defending Data: New Colorado Law Creates Stricter Obligations for Handling Data Breaches, Disposal, and Security

Publication — 06/05/2018

Last week, Governor John Hickenlooper signed a bill with wide ranging implications for any entity that collects and maintains the personal information of Colorado residents. The law, which goes into effect on September 1, 2018, significantly bolsters the state's data breach notification requirements for both private and governmental entities and puts in place new security and data disposal obligations. As with the original Colorado state data breach law, the state attorney general has the authority to bring an action against a violator to ensure compliance and/or to recover direct economic damages resulting from the violation.

Updated Data Breach Obligations

The new law expands an entity's obligations in the event of a data breach. Entities must now notify all affected Colorado residents within 30 days of the date of determination that a breach has occurred, and they must also notify the Colorado attorney general within the same time period if the breach is reasonably believed to have affected 500 or more Colorado residents. The definition of personal information has also been expanded to include, among other things, health information and information that would permit a third party to access an individual's user account (e.g., username plus security questions or password).

In addition to a broader definition of personal information and a stricter timeline for data breach notification, the new law has specific content requirements for a data breach notification. Any notification must include: (i) the date (or date range) of the breach, (ii) a description of the personal information that was acquired or is believed to have been acquired, (iii) contact information for an individual's further inquiries, (iv) contact information for consumer reporting agencies, (v) contact information for the FTC, and (vi) a statement that the individual may obtain information about fraud alerts and security freezes from the FTC or credit reporting agencies.

Data Disposal Plans and Security Obligations

The new law also requires entities to create a written policy for the destruction or disposal of documentation containing personal information. These plans must require that such documentation be destroyed when no longer needed.

Additionally, entities are required to maintain reasonable security practices given the nature of the information being collected and the entity's size and operations. It is important to note that these obligations are not limited solely to the entity. Each entity must also pass these obligations down to

any third-party service providers that process personal information on their behalf, which will require updates to vendor agreements where these provisions are not already included.

In light of this new law, any entity doing business in, or processing data of residents in, Colorado would be wise to review its current policies. Some requirements, including the tight deadline for data breach notification and flow-down of security obligations to contractors, could require further preparation and planning before September 1st.