Colorado Reaches New High with Strict Data Breach Notification Law

Dana B. Rosenfeld, Alysa Z. Hutnik

June 11, 2018

On May 29, Colorado Governor John Hickenlooper signed into law HB18-1128 to strengthen data breach notification requirements for companies and government entities collecting and maintaining personal information from Colorado residents.

Effective September 1, covered entities will be required to notify individuals within 30 days of discovery of a security breach, unless the entity is notified that such a disclosure will impede a criminal investigation. Existing law requires notification to be made “in the most expedient time possible, and without unreasonable delay.” Republican state representative and bill co-sponsor Cole Wist stated the term “reasonable” was "too subjective and loose," and could prevent consumers from acting quickly to prevent identity theft. This makes the new law one of the strictest data breach notification laws in the country. The following identifies pertinent changes to existing law.

Mandatory Information Security Procedures or Programs

Businesses must implement “reasonable" information security procedures or programs to protect the personal data they have - including data that has been shared with third parties - from unauthorized access, use, modification, disclosure, or destruction. Businesses that maintain paper or electronic documents containing customer personal information must develop a written policy for the destruction of such documents once they are no longer needed.

Expanded Definition of PI

Personal information currently is defined as a resident’s first name or initial and last name in combination with certain common data elements, including SSN, driver’s license number, or credit card account number. The new law broadens the definition of personal information to include, among other things, the combination of a username and password, or security questions and answers that would permit access to an online account.

Notification Content Requirements

Existing law is silent on the content of notification letters to consumers. The new law requires that notification include the following information:

- The date, estimated date, or date range of the breach;
- A description of the information that was acquired;
- Contact information for the entity so the resident can inquire about the breach;

- Toll free numbers for consumer reporting agencies and the FTC; and
- A statement informing residents that they can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes.

Notification to Regulators

Existing law contains a notification requirement to CRAs for breaches affecting at least 1,000 residents. The new law imposes an additional notification requirement to the Colorado Attorney General within 30 days of discovery for breaches affecting at least 500 residents.

By this new legislation, Colorado joins a handful of states mandating the implementation of a reasonable information security program. We will continue to monitor legislative activity surrounding breach notification.

Summer associate Vishwani Singh contributed to this post. Ms. Singh is not a practicing attorney and is practicing under the supervision of principals of the firm who are members of the D.C. Bar.