# IMA CLIENT ALERT

Developed with Ballard Spahr LLP

## COLORADO BREACH LAW: IMPLEMENTING AND MAINTAINING REASONABLE SECURITY PROCEDURES FOR COVERED ENTITIES

**Colorado has enacted groundbreaking privacy and cybersecurity legislation that will require covered entities to implement and maintain reasonable security procedures, dispose of documents containing confidential information properly, ensure that confidential information is protected when transferred to third parties, and notify affected individuals of data breaches in the shortest time frame in the country.** The new law was spearheaded by the Colorado Attorney General's office, which is charged with enforcing its requirements. As a result of the legislation, covered entities should consider implementing written information security programs, third party vendor management controls, and incident response plans to best position themselves against potential enforcement actions and civil litigation in the future.

Notable provisions of the new law are as follows:

### DATA SECURITY REQUIREMENTS

For the first time, covered entities that maintain, own or license "personal identify information" (PII) of a Colorado resident are required to implement and maintain reasonable security procedures and practices that are "appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

The law defines PII broadly to include a social security number; personal identification number; password; pass code; official state or government-issued driver's license or identification card number; government passport number; biometric data; employer, student or military identification number; or financial transaction device (as defined in C.R.S. § 18-5-701(3)).

Covered entities also must take measures to protect PII when transferring it to third parties. Unless a covered entity agrees to provide its own security protection for the information it discloses to a third-party service provider, the covered entity "shall require" the third-party service provider to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII disclosed and reasonably designed to help protect the PII from unauthorized access, use, modification, disclosure, or destruction. A "third-party service provider" is defined as an entity that "has been contracted to maintain, store, or process personal information on behalf of a covered entity."

The Attorney General's office is authorized to enforce these new requirements and may bring an action in law or equity to ensure compliance or recover direct economic damages resulting from a violation.

## CHANGES TO COLORADO'S BREACH NOTIFICATION LAW

The new law strengthens and expands Colorado's data breach notification law. Perhaps the most significant change is that covered entities now **must notify affected individuals within 30 days after determining that a security breach occurred that resulted in, or is likely to result in, misuse of personal information.** Colorado's 30-day deadline is the shortest of any state. Florida also has a 30-day deadline but allows for an additional 15 days under certain circumstances.

**The law will become effective on September 1, 2018.**

## INSURANCE CONSIDERATIONS

If you currently purchase Cyber insurance coverage, make certain you are familiar with the policy features and requirements. Specifically, many policies require use of vendors designated by the carrier to assist you. Request and review a list of those vendors and identify providers you would like to engage. If possible, organize an introductory call or meeting. As part of the process, have a draft engagement letter organized that if or when you need to engage, you are prepared.

If you not currently purchase Cyber insurance, you want to re-consider. Based on the short window for investigation and notice, it will be essential to have access to experts to help navigate those obligations. Most Cyber policies will provide you with immediate access to legal counsel (aka breach coach), forensic investigator, public relations and written notification providers. The policies will also fund any defense costs, damages, fines and penalties associated with a breach.

**TIM BURKE**
IMA, Inc. | Director Cyber Risk
*tim.burke@imacorp.com*

**DAVID STAUSS**
Ballard Spahr | Partner
*staussd@ballardspahr.com*