Protecting Personal Identifying Information In Colorado – The Rules Have Changed

By Lauren M. Collins, Esq., Burns, Figa & Will, P.C.

&

Jeremy Schupbach, Director, Legislative Relations, Colorado Bar Association

On September 1, 2018, Colorado House Bill 18-1128 ("HB 1128") went into effect. HB 1128 essentially heightens Colorado covered entities' obligations to implement plans to protect and destroy personal identifying information ("PII") they maintain, own or possess. HB 18-1128 creates a number of new expectations and definitions for which lawyers, and the clients they advise, must be aware.

As a result of HB 1128, C.R.S. § 6-1-713(2)(b) now defines PII to mean: "a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in section 6-1-716 (1)(a); an employer, student, or military identification number; or a financial transaction device, as defined in section 18-5-701(3)."

HB 1128 modified the term "covered entity" in C.R.S. § 6-1-713(2)(a) to more broadly include any individual, corporation, partnership, limited liability company or any other legal or commercial entity "that maintains, owns, or licenses [PII] in the course of the person's business, vocation, or occupation." Each of us in Colorado, from solo practitioners to large entities, should assume that the we, or the business we operate is a "covered entity" and that we are responsible for compliance. A key point here is that the legislature did not define "maintain" making it unclear whether the intent is to include simple possession of PII (which could be broadly interpreted to include an email correspondence unread in your inbox) or PII actually curated and kept by covered entities. A court would likely look to the dictionary definition of "maintain," which one could conservatively read to require more than passive possession. However, when developing a written policy, it may be prudent to go beyond the dictionary definition while not drafting the policy to be so inclusive that it cannot be complied with.

Previously, the state's PII definition applied to "each public and private entity . . . that uses documents during the course of business that contain [PII]", and required that each such entity "develop a policy for the destruction or proper disposal of paper documents containing PII."

As a result of HB 1128, covered entities that maintain, own or license PII of Colorado residents must do more than merely "develop a policy for the destruction or proper disposal of paper documents containing PII." This new definition now applies whether or not the entity is organized under Colorado law or even doing business in Colorado. Under HB 1128, each covered entity must:

1. Develop written policies for the destruction and maintenance of PII, and

2. Implement and maintain reasonable security procedures and practices to safeguard PII

To look more closely at these two basic requirements:

> "[D]evelop a **written** policy for the destruction or proper disposal of **those** paper **and electronic** documents containing PII."

In describing the written policy, C.R.S. § 6-1-713(1) requires that the written policy must require that PII in its control or possession be destroyed, or the covered entity must arrange for the destruction of the PII when the PII is "no longer needed." "Destruction" is defined by reference to "shredding, erasing or otherwise modifying the PII to make it unreadable or undecipherable through any means."

In addition to developing the required written policy, C.R.S. § 6-1-713.5(1), each covered entity that maintains, owns, or licenses PII "of an individual residing in [Colorado]" must:

> "[I]mplement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the business and its operations."

This clearly gives smaller businesses the right to scale their compliance – but any loss or unauthorized access to PII will likely result in greater liability to the smaller business with less access to cutting edge protection, than it would to a larger business that has the ability to allocate more funds to purchase more robust protection. The intention of the proponents of HB 18-1128 was to create a living law that is continuously updated through case law, and therefore is intentionally left broad and open to interpretation, both by covered businesses and entities, as well as by the Attorney General.

A covered entity may contract with a third-party service provider to maintain PII on its behalf. This may include a 401(k) provider, a payroll company, or other third-party service provider. That does not, however, let the covered entity off the hook. C.R.S. § 6-1-713.5(2) requires that the covered entity contracting with the third-party service provider:

> [S]hall require that the third-party service provider implement and maintain reasonable security procedures and practices that are:
>
> (a) Appropriate to the nature of the [PII] disclosed to the third-party service provider; and
>
> (b) Reasonably designed to help protect the [PII] from unauthorized access, use, modification, disclosure, or destruction.

Thus, the covered entity is potentially liable for breaches resulting from a third-party service provider's action (or inaction) unless the covered entity can show that it accomplished the appropriate due diligence – and we do not know what that term means. Should each covered entity obtain a certification from each third-party service provider each year? The vague language provides some necessary latitude, but should not be interpreted as a "safe harbor" should a breach occur. Until the courts have had an opportunity to interpret the statute, best practice would be to approach this in the most conservative manner keeping the legislative intent in mind when developing policies and procedures.

C.R.S. § 6-1-713(3) and § 6-1-713.5(4) provide that a covered entity that is regulated by state or federal law and that maintains procedures for disposal of PII that complies with the guidance established by the applicable state or federal regulator "is in compliance with this section."

In a provision that is among the most stringent in the United States, C.R.S. § 6-1-716(2) now provides that any covered entity must give notice of a breach of PII security "to the affected Colorado residents" "not later than thirty days after the date of determination that a security breach occurred" unless the covered entity determines, after conducting "in good faith a prompt investigation" and the covered entity "determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur." It is important to note that where a covered entity does not even know that a

breach has occurred for a period of time, it is still required to notify affected Colorado residents within thirty days of the breach. If that period does not leave sufficient time for the covered entity to conduct a good faith investigation, then notification to all Colorado residents should be made. C.R.S. § 6-1-716(2)(f) also requires the covered entity to notify the Colorado attorney general of the breach.

"Notice" is broadly defined in C.R.S. § 6-1-716(1)(f) to include any of a list of, and sometimes a combination of, methods to notify customers or clients, including mail, telephone, email, posting "conspicuously" on a website or in a "major statewide media." Notice must be made by the covered entity "in good faith, in the most expedient time possible and without unreasonable delay" and without charge to the affected persons. C.R.S. §§ 6-1-716(2)(a.5) and -716(c). If more than 1,000 Colorado residents are involved in the data breach, C.R.S. § 6-1-716(d) requires that the covered entity "also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis."

As now required in C.R.S. § 6-1-716(2)(a.2), the notice must contain information about the date/dates of the breach, a description of the PII that was subject to the breach, and various methods by which the Colorado residents subject to the breach can obtain more information. Where passwords and similar access points are thought to be compromised, C.R.S. § 6-1-716(2)(a.3)(1) requires the notice also contain direction to the recipients to change passwords and other log-in credentials.

Notice to the affected persons may only be delayed "if a law enforcement agency determines that the notice will impede a criminal investigation" and the agency "has notified the covered entity . . . not to send notice."

HB 1128 also added article 73 to Title 24 imposing similar requirements on Colorado governmental agencies who have and now must protect PII.

All covered entities – and that generally means all of us – that maintain, use or license PII of Colorado residents should evaluate their data protection and data breach policies. Covered entities are not only entities located in Colorado or that are formed under Colorado law, but are defined without geographic limitation in C.R.S. § 6-1-102(6) – but only with respect to whether the PII being maintained relates to Colorado residents.

- If any covered entity (not exempt because of the federal or state law requirements found in C.R.S. § 6-1-713(3) and § 6-1-713.5(4)) do not have written policies in place, they should be implemented in order to comply with the heightened obligations.

- Having policies is not, however, the only answer. Appropriate procedures have to be established to maintain the security and integrity of that PII – both in house at the covered entity and at the covered entity's third-party service providers.

This is a new law, and there is much to be interpreted. Nevertheless, as set forth in the September 7, 2018, *Denver Business Journal* (article entitled *Consumer data 'stakes are higher'* by Andrew Dodson at Page A17), the stakes are now much higher for companies doing business with Colorado residents involving PII, and the legislation requiring "reasonable security procedures" was "written vaguely on purpose." Whether that vagueness helps the smaller business owner to downsize some requirements, or some degree of strict liability will be applied remains to be seen. At this time there is no best practice or guidance available to entities now covered under HB 1128. With time and case law developments, the best practices will become more evident. In the meantime, according to proponents of the legislation, you should "write

policies you can be proud of, and in the event of a data breach be able to demonstrate to the Attorney General that you have created policies, procedures and documents that demonstrate you took this seriously and thought through the issue."