THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

JOSHUA DIAMOND
DEPUTY ATTORNEY GENERAL

SARAH E.B. LONDON
CHIEF ASST. ATTORNEY GENERAL

TEL: (802) 828-3171

ago.vermont.gov

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER
05609-1001

April 27, 2020

Re: *Recent Changes to Vermont's Security Breach Notice Act, 9 V.S.A. § 2435*

To Whom it May Concern:

RECENT CHANGES TO VERMONT'S SECURITY BREACH NOTICE ACT

You should be aware of recent changes to Vermont law regarding data privacy and security. These amendments take effect on July 1, 2020.

On March 5, 2020, Governor Scott signed Bill S.110 of the 2019/20 Legislative Session. This created substantive amendments to Vermont's Security Breach Notice Act, 9 V.S.A. §§ 2330 & 2335, and enacted a "Student Online Personal Information Protection Act" similar to the law first enacted in California and later adopted by over 20 states. 9 V.S.A. §§ 2443 to 2443f.

The Security Breach Notice Act changes include an expansion of the definition of Personally Identifiable Information, an alternate notification process for login credentials, and a change to substitute notice requirements.

Personally Identifiable Information ("PII")

Prior to this amendment, the definition of PII in Vermont contained the traditional four elements when unencrypted, a consumer's first name or first initial and last name in combination with:

- Social Security number;
- Driver license or nondriver identification card number;
- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; or
- Account Passwords, personal identification numbers, or other access codes for a financial account.

The new law includes these elements, and adds when combined with a consumer's first name or first initial and last name:

- Individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
- Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- Genetic information; and
- Health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional's medical diagnosis or treatment of the consumer; or a health insurance policy number.

The notification requirements for the above PII remains substantively the same.

These definitions were arrived at after hearing from several stakeholders and followed the intent of the legislature to provide the broadest amount of consumer protection while taking into account the concerns of certain business actors.

The biometric data language is based on that used in Oregon's breach act, though Vermont's definition varies somewhat:

> Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction.

Health Information

The health information language was the result of significant discussion and debate, during which definitions from Oregon and Delaware were considered. The first part is intentionally broad. It includes "Health records," or "records of a wellness program or similar program of health promotion or disease prevention." Health records are not necessarily limited to records maintained by a health provider or other HIPAA-covered entity. They could include, for example, information about an individual's health maintained by a business or a data broker.

However, where a data collector has complied with its notice obligations under HIPAA and the security breach *only* pertains to health information, then the data collector is deemed to be in compliance with Vermont's statute.[1]

Login Credential Breach

"Login credentials" are defined as "a consumer's username or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account." Login Credentials are not part of the definition of PII, but most sections of the law that used to refer to PII now refer to PII "or login credentials." In other words, when determining whether a breach took place or whether a business has a duty to notify generally, consider login credentials the same as you would consider PII.

Where login credentials differ from PII is in *how* notice is to take place. With one significant exception, the new language regarding login credential notification, which is based strongly on the California law's requirements, is as follows (subdivision (b)(6) refers to the traditional notification options):

> 2453(d)(3) If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods specified in subdivision (b)(6) of this section and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials.
>
> (4) If a security breach is limited to an unauthorized acquisition of login credentials for an email account:
>
> > (A) the data collector shall not provide notice of the security breach through the email account; and
> >
> > (B) the data collector shall provide notice of the security breach through one or more of the methods specified in subdivision (b)(6) of this section or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account.

[1] 2453(e). A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if:
(1) the data collector experiences a security breach that is limited to personally identifiable information specified in 2430(10)(A)(vii); and
(2) the data collector provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D.

One distinguishing factor of Vermont's law is that, in the event of a credential breach, *still* has the obligations to provide notice to the Attorney General: both the 14-day Preliminary Notice, and notice at the time that consumers are notified, pursuant to 9 V.S.A. § 2435(b)(3).

Stakeholders were concerned about the scenario where an unauthorized user steals login credentials from an *unrelated party* and uses those credentials to log in to a consumer's account controlled by the data collector. This situation is not intended to trigger credential breach notification obligations by the data broker (though the unrelated party would have such obligations). Where the credentials are stolen from the data collector, however, the new notice obligations apply. In response to this concern, the following language was added for clarification:

> 2435(b)(3)(D) If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.

Note that this exception only applies to situations where the breach only involves login credentials and not other PII.

Substitute Notice

Finally, the threshold for permitting substitute (as opposed to direct) notice has changed. Vermont's substitute notice requirements permit a data collector to comply with its notice obligations in the event of a PII breach by "conspicuously posting the notice on the data collector's website if the data collector maintains one and notifying major statewide and regional media." 9 V.S.A. § 2435(b)(6)(B).

Previously, substitute notice was permitted where the cost of Direct Notice via writing or telephone would exceed $5,000, more than 5,000 consumers would be receiving notice, or the data collector does not have sufficient contact information.

Now, substitute notice is only permitted where the *lowest* cost of providing Direct Notice via writing, email, or telephone would exceed $10,000, or the data collector does not have sufficient contact information. It is no longer permitted to provide substitute notice where the number of consumers exceed a certain threshold.

In other words, if the data collector has the contact information of affected consumers (whether residential address, email address if this is the primary method of communication with the consumer, or telephone number), and the data collector is able to provide Direct Notice via one of those methods for a total amount of $10,000 or less, the data collector must provide Direct Notice.

Conclusion

We understand the complexity of security breach notice acts, and the challenge complying with the laws of 50 states plus territories. As usual, we remain open to calls where businesses or their counsel require clarification of our laws. In addition, recall that the "preliminary notice" need not involve significant details, or even absolute certainty that a breach has occurred. It is simply a "heads' up" that a significant data incident has occurred that may turn out to be a breach, and it is a good way to demonstrate early in the process your commitment to complying with the law.

Sincerely,

/s/ Ryan Kriger

Ryan Kriger
Assistant Attorney General
Public Protection Division