Bloomberg BNA

Privacy and Security Law Report®

Vermont Offers Businesses Two Confusing Options For Notifying the Vermont AG of Security Breaches

By Nathan D. Taylor

Last year, Vermont amended its security breach notification law[1] to join the growing list of states that require notice to the state attorney general or other state regulator regarding security breaches.[2] Unlike other states, Vermont offered businesses two options with respect to how and when notice must be provided to the Vermont attorney general (AG). These options are based on whether a business has made a sworn affirmation to the AG regarding its information security practices. This article describes the Vermont AG notice requirement (as well as the AG's interpretation of this requirement), the sworn affirmation form issued by the AG, and the pros and cons associated with making the sworn affirmation.

As discussed in greater detail below, a business has two options with respect to notifying the AG of a security breach:

Option 1—If a business experiences a covered security breach and the business has *not* provided the AG with a sworn affirmation regarding its information security practices, the business must:

1. within 14 business days of discovering the breach or providing notice to consumers (whichever is sooner), provide the AG with notice that includes, among other things, a description of the breach; and

2. when providing notice to Vermont residents, also provide the AG with the number of Vermont residents affected and a copy of the letter provided to consumers.

Option 2—If a business has provided the AG with a sworn affirmation regarding its information security practices and then experiences a covered security breach, the business must:

1. prior to providing notice to Vermont residents, provide the AG with notice that includes, among other things, a description of the breach; and

2. when providing notice to Vermont residents, provide the AG with the number of Vermont residents affected and a copy of the letter provided to consumers.

As discussed below, Option 2 provides a business with additional time to notify the AG of a breach (*i.e.*, a ''carrot'' for making the sworn affirmation). Ultimately, a business must weigh each option. Whether it is advantageous for a business to file a sworn affirmation is open to debate.

The Vermont Breach Amendment

On May 5, 2012, the Vermont governor signed into law a bill that included a provision amending the Vermont breach law to add a requirement to notify the Ver-

[1] Vt. Stat. Ann. tit. 9, §§ 2430, 2435. The Vermont law may be found at http://www.atg.state.vt.us/assets/files/Security%20Breach%20Notice%20Act.pdf.

[2] It is important to note that, in general, the Vermont AG notice requirement applies to any business that is subject to the Vermont breach law; that is, any business that owns or licenses computerized personal information that includes covered types of personal information relating to a Vermont resident that experiences a breach involving that information. Certain types of entities, however, are exempt from the AG notice requirement. Specifically, the AG notice requirement does not apply to a person who is licensed or registered under Title 8 of the Vermont Code by the Vermont Department of Financial Regulation. In addition, a financial institution that is subject to the breach response program guidance issued by the federal banking agencies to implement the Gramm-Leach-Bliley Act is exempt from the Vermont breach law, including the AG notice requirement.

Nathan D. Taylor is an associate with the Washington office of Morrison & Foerster LLP, where he concentrates on assisting clients in managing consumer information, including customer and employee information, and developing procedures, practices, and other solutions to comply with complex privacy and information security laws.

mont AG of security breaches.[3] The amended law is far from a model of clarity. In addition, the AG has issued its own, equally confusing guidance interpreting the mechanics of this notice process (Guidance).[4]

Option 1—A Business Does Not Provide the Sworn Affirmation

The amended law provides that if a business experiences a breach, the business must provide notice of the breach to the AG within 14 business days of discovering the breach or when the business provides notice to consumers (whichever is sooner).[5] This notice must include the date of the breach, the date of discovery of the breach, and a ''preliminary'' description of the breach.[6] The Guidance describes this notice as a ''preliminary notice'' and one that should be provided to the AG ''[w]ithin 14 days'' of discovering the incident.[7] As a result, the Guidance reads out of the statute the word ''business'' from ''14 business days.'' In addition, the Guidance eliminates as a benchmark the time when notice is provided to Vermont residents from the determination of when notice is required to the AG.

Separately, the amended law provides that ''[w]hen'' a business provides notice of the breach to Vermont residents, the business also must notify the AG of the number of Vermont residents affected, if known, and provide a copy of the letter provided to Vermont residents.[8] The Guidance interprets the statute's plain language with respect to timing quite differently. Specifically, the Guidance indicates that a business must provide the AG with: (1) a copy of the consumer notice ''[p]rior to notifying'' Vermont residents of the breach; and (2) the number of Vermont residents affected by the breach ''[w]hen notifying'' Vermont residents.[9] This deviation from the statutory language with respect to the timing of providing the AG with a copy of the consumer notice appears clear: the Guidance indicates that the AG ''may offer suggestions as to how the notice can be improved or brought into compliance.''[10]

Option 2—A Business Provides the Sworn Affirmation

The amended law provides a second option. Specifically, the law provides that a business, which, prior to a breach, has sworn in writing to the AG (on a form and in a manner prescribed by the AG) that it maintains written policies and procedures to maintain the security of personal information and to respond to a breach in a manner consistent with Vermont law, may notify the AG of the breach prior to providing notice to consumers (as opposed to notifying the AG within 14 business days of discovery).[11] This notice must include the date of the breach, the date of discovery of the breach, and a description of the breach.[12] Separately, as discussed above, ''[w]hen'' a business provides notice of the breach to Vermont residents, the business also must notify the AG of the number of Vermont residents affected, if known, and provide a copy of the letter provided to Vermont residents.[13]

Oddly, the Guidance seems to read out of the statute the obligation to provide the AG with the ''first'' notice that includes, among other things, a description of the breach. That is, the Guidance could be read to require a business that has provided the sworn affirmation only to provide the AG with a copy of the consumer letter and the number of Vermont residents affected by the breach.

The Vermont AG Affirmation Form

The AG recently made available the affirmation form that a business may provide to the AG in order to ''waive'' the 14-business-day ''preliminary'' notice to the AG.[14] The affirmation form indicates that by submitting the sworn affirmation, the employee of the business is ''averring that the [specified] facts are true subject to penalties of perjury.''

Specifically, the form is comprised of the following seven ''affirmations'':

1. the individual providing the sworn affirmation has read the Vermont breach law (or legal counsel has explained the law to the individual);
2. the individual's business has written policies and procedures to ''maintain the security'' of personal information collected by the business;
3. the business also has written policies and procedures to respond to a security breach in a manner consistent with the Vermont breach law;
4. the individual has authority to ensure that the these policies and procedures are properly ''implemented'';
5. the individual understands that the Vermont breach law requires the business to notify Vermont residents of a breach as expeditiously as possible and without unreasonable delay, but not later than 45 days after discovery or notification of the breach;
6. the individual understands that the Vermont breach law requires the business to notify the AG of a breach before notifying Vermont consumers, but that the duty to provide the AG notice within 14 business days of discovering the breach is waived by the AG if the business provides this affirmation; and
7. the individual understands that the Vermont breach law is enforced under the state's Consumer Protection Act (Vt. Stat. Ann. tit. 9, §§ 2451–2466), which permits

---

[3] Text of H. 254, as approved, is available at http://www.leg.state.vt.us/docs/2012/Acts/ACT109.pdf (11 PVLR 919, 6/11/12).

[4] Office of the Attorney General of Vermont, Attorney General Security Breach Notification Guidance (updated July 26, 2012) [hereinafter Breach Notification Guidance], *available at* http://www.atg.state.vt.us/assets/files/Security%20Breach%20Guidance.pdf.

[5] Vt. Stat. Ann. tit. 9, § 2435(b)(3)(A)(i).

[6] *Id.*

[7] Breach Notification Guidance, *supra* note 4, at 4.

[8] Vt. Stat. Ann. tit. 9, § 2435(b)(3)(B)(i). A business also can provide a second copy of the letter to Vermont residents from which the types of personal information subject to the breach are redacted and which the Vermont AG will use for public disclosure purposes. *Id.* § 2435(b)(3)(B)(ii).

[9] Breach Notification Guidance, *supra* note 4, at 4.

[10] *Id.* at 1.

[11] Vt. Stat. Ann. tit. 9, § 2435(b)(3)(A)(ii).

[12] *Id.*

[13] *Id.* § 2435(b)(3)(B)(i). A business also can provide a second copy of the letter to Vermont residents from which the types of personal information subject to the breach are redacted and which the Vermont AG will use for public disclosure purposes. *Id.* § 2435(b)(3)(B)(ii).

[14] Office of the Attorney General of Vermont, Vermont Attorney General's Security Breach 14-Day Preliminary Notice Affirmation, *available at* http://www.atg.state.vt.us/assets/files/2012-06-29%2014-day%20Affirmation.pdf.

  PVLR ISSN 1538-3423

> penalties not to exceed $10,000 per violation and that each consumer affected and each day of noncompliance is a separate violation.

The AG's form does not allow the individual making the sworn affirmation (or her business) to modify the affirmations included in the form.

Practical Implications for Businesses

With this confusing statutory backdrop and the AG's equally confusing interpretation of the statute, businesses will be left with the decision of whether to provide the sworn affirmation. The following highlights some of the potential pros and cons associated with making the sworn affirmation to the AG.

The ''Pros''

Additional Time—Depending on the nature of the incident, a business that has provided the sworn affirmation may be able to obtain approximately 4 additional weeks' time before being required to notify the AG of a breach (assuming that notice to Vermont residents is not provided until the end of the statutory 45-day notification time period).

The Need for More Time—In some instances, the benefit of additional time cannot be overstated. For an incident where a forensic or other investigation is taking more time than expected or where the business is still attempting to determine the facts regarding the incident, having additional time to notify the AG can only be beneficial.

For example, if a business discovers an incident and immediately begins investigating the incident, the business will be put in a difficult position if, within 14 business days after discovering the incident, the business cannot yet confirm whether the incident qualifies as a noticeable breach under the Vermont breach law. Similarly, if a forensic or other investigation is ongoing when a business notifies the AG within the 14-business-day time period but, after providing the notice, the investigation concludes that the incident is not covered by the Vermont law, the business may have to justify to the AG why notice is not required to Vermont residents.

That is, by providing the AG with a ''preliminary'' notice of an incident, a business may create the presumption that the incident is covered by the Vermont law. In such an instance, additional time to complete its investigation would prove beneficial for a business.

Potential Ability to Merge Notifications Into a Single Notice—Because of the additional time afforded by having made the sworn affirmation (*i.e.*, not being required to notify the AG until prior to notifying Vermont residents), a business may be able to merge the two notice obligations into a single notice (provide a single notice to the AG that includes all the elements of the Option 2 notices described above).

The Affirmation Is High Level—The substance of the sworn affirmation with respect to information security practices is high level. A business must only indicate that it has written policies and procedures to ''maintain the security'' of personal information collected by the business and to respond to a breach in a manner consistent with Vermont breach law.

While this raises factual questions about whether a business actually maintains such policies and procedures, businesses who have designed their information security policies and procedures to comply with applicable law should be able to make such affirmations. Importantly, the substance of these two affirmations does not identify specific information security practices that a business must maintain (*e.g.*, encryption).

The ''Cons''

The Additional Time Will Not Always Be Available—The benefit of obtaining additional time to notify the AG of a breach will be incident-specific. Under both the 14-business-day notice requirement and the ''delayed'' option after providing a sworn affirmation, notice to the AG always must be provided before notifying Vermont residents of an incident. As a result, the actual amount of additional time that a business obtains before having to notify the AG will depend on when Vermont residents ultimately will be notified. For example, if a business notifies Vermont residents within 10 days of discovering a breach, the business must provide the AG with notice prior to notifying the Vermont residents even if the business had completed the sworn affirmation.

Who Signs the Affirmation—The individual making the sworn affirmation must have the authority to ensure that the business's information security policies and procedures are properly ''implemented.'' This fact may limit those individuals within a business who can make the sworn affirmation to a few executives or senior management within specific departments or business units. Moreover, it is not clear whether the sworn affirmation will continue to be valid if the individual making the affirmation later leaves the business (*i.e.*, would the business be required to make a new affirmation?).

Perjury Is a Significant Penalty—With respect to the individual making the sworn affirmation, perjury as a potential penalty is quite significant. If an individual makes the sworn affirmation and her business is later found to have failed to maintain appropriate information security policies and procedures, would the AG bring a perjury charge against the individual? Would there only be a risk of a perjury charge where the individual and the business had been willfully and knowingly disregarding information security and the significance of the sworn affirmation?

Additional Element in an Enforcement Action—If a business has made the sworn affirmation but the business does not maintain the types of information security policies and procedures included in the affirmation, it is possible that the sworn affirmation could provide an additional element in an enforcement action against the business relating to a failure to maintain appropriate information security policies and procedures. That is, in the context of an investigation or enforcement action by the AG, a failure to maintain appropriate information security policies and procedures would only be compounded by the fact that the business had submitted a sworn affirmation indicating that it was maintaining appropriate policies and procedures.

In the end, each business covered by the AG notification requirement must weigh these pros and cons. Regardless of its decision, notice(s) to the AG will be required for a covered security breach involving personal information regarding Vermont residents.

In addition, if a business experiences a security incident that it believes requires notice to consumers in other states, the business also must consider whether any other state requires notice to a state attorney general or other state entity (*i.e.*, one of the sixteen states in addition to Vermont with a state notice requirement).

As always, businesses should be cognizant of the ever-changing state landscape and new amendments to existing state laws.

   ISSN 1538-3423