Blackbaud Breach Q & A for Businesses, Nonprofits, and Legal Counsel:

In mid-July, Blackbaud, a software provider used by a significant portion of the nonprofit community, reported a ransomware attack that took place in May 2020 and resulted in the acquisition of data by cybercriminals. According to public statements, Blackbaud claims that it has "no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly," but, to date, has not announced any concrete substantiation of this claim. It is generally difficult to "prove" that a cybercriminal that has acquired sensitive data has deleted it, and absent affirmative proof, one should treat that data as "acquired" or breached under Vermont's laws.

The Attorney General's Office (AGO) is encouraged by how quickly users of Blackbaud's software have moved to ensure compliance with Vermont and other states' Security Breach Notice Acts by issuing notices to their customers, donors, and others. This Q & A attempts to address some issues that have arisen and provides suggestions based on information that is currently publicly available. The details of this incident, however, may develop over time.

What is considered a security breach?

An incident is only considered a "security breach" if (i) the subset of data defined as "Personally Identifiable Information" or "PII" is acquired, and (ii) that data is unencrypted. Blackbaud's public statement is that that no unencrypted credit card information, bank account information, or Social Security numbers were acquired. While these are the most common types of PII implicated, Vermont law also includes other data as PII:

- government identification numbers like drivers' licenses and passports;
- health information, including health insurance policy numbers;
- genetic information;
- biometric information; and,
- login credentials.

The AGO is not aware that Blackbaud has commented on these data types.

If a nonprofit has entered any PII, like a Social Security number, into an otherwise unencrypted field, like a freeform text field, that information should be assumed to have been acquired, resulting in a breach.

A full explanation of Vermont's Security Breach Notice Act can be found in this recently issued guidance.

Is Vermont's Breach Notice Act the right state's law to comply with?

Organizations should comply with Vermont's Act with regard to all consumers affected by the breach who reside in Vermont. If an organization must notify anyone outside of Vermont, it must comply with the law of the state in which the consumer resides.

How should a Blackbaud user respond to this incident?

Many organizations appear to be issuing notice without clarifying whether or not a consumer's PII was affected. While the AGO appreciates the desire for transparency, notices like this, particularly coming from multiple sources as is occurring here, can create anxiety without providing needed clarity to consumers:

If an organization knows with certainty that it *has not* stored any PII in a Blackbaud system, or has only stored it in fields that Blackbaud claims to be encrypted, then that organization has *not* experienced a security breach and has no obligation under Vermont law to issue notice.

If an organization is uncertain of this fact, and cannot confirm one way or the other, it should treat this as a security breach and follow the Vermont Security Breach Act Notice Guidance.

Is a Blackbaud user required to issue notice if no PII was breached?

The AGO understands that many organizations wish to be as open as possible with customers and donors, and may want to issue notice even if no PII was affected. Some information stored in the Blackbaud database, like home values, income levels, or even personal preferences, is not considered PII but would still be the sort of information that many consumers would like to know has been accessed.

If an organization is certain that a breach as defined by the law has *not* occurred (that is, unencrypted PII was not involved), but still wishes to issue notice, the AGO encourages you to be as clear as possible. This may include the following elements, but, again, note that none of this is obligatory.

- Explain that the customers, donors, or others may have heard about the Blackbaud breach.
- State that, based on representations from Blackbaud no PII was acquired, if applicable.
- If there are pieces of sensitive information that are not PII involved, you may want to disclose those. None of this is obligatory. We are recommending this to avoid notices that people may find confusing.
- Include a warning that "phishing" scams often occur in the wake of a breach and that you will not call or email the consumer asking them for their login credentials, credit card number, or other financial information. Furthermore, you do not accept payment in the form of gift cards and would never request them.

If a notice of "non-breach" is being issued, the AGO does not need to be informed of it. Breach notices, as usual, must be sent to the AGO, where they are posted on its website.

If you have any questions or are uncertain about anything in the guidance, please contact ago.securitybreach@vermont.gov or 802-828-5479.