blackbaud

Constituent Response Toolkit

Table of Contents

Background for Customers

THE CYBERCRIME INDUSTRY REPRESENTS AN OVER TRILLION-DOLLAR INDUSTRY THAT IS EVER-CHANGING AND GROWING ALL THE TIME—A THREAT TO ALL COMPANIES AROUND THE WORLD. AT BLACKBAUD, OUR CYBER SECURITY TEAM SUCCESSFULLY DEFENDS AGAINST MILLIONS OF ATTACKS EACH MONTH AND IS CONSTANTLY STUDYING THE LANDSCAPE TO ENSURE WE ARE ABLE TO STAY AHEAD OF THIS SOPHISTICATED CRIMINAL INDUSTRY.

In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. This incident did not involve solutions in our public cloud environment (Microsoft Azure, Amazon Web Services), nor did it involve the majority of our self-hosted environment. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. We have built this step-by-step toolkit in the event you and your organization determine that you need to notify your constituents. The following toolkit should be used to ensure that you are taking the right steps in communicating efficiently and effectively with your constituents.
We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in this toolkit to make it easier.

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. We apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

If you have any questions, please contact the dedicated team we have established for this incident:

- **North and South America**: 1-855-907-2099 between 9 a.m. and 9 p.m. ET Monday – Friday

- **Europe/UK**: 0800 307 7591 **or** +44800 307 7591 (when called from outside of UK) 24 hours/day
- **Australia and Asia**: Please email Jenny.Bloch@blackbaud.com

Steps for Assessing if You Need to Notify Your Constituents

The following summary does not constitute legal advice on any particular facts or circumstances. Please consult with your organization's legal counsel to determine which laws apply to you and what your responsibilities are.

Your organization was sent an email and direct mail letter with the name of the solution(s) that were part of this incident. We sent the email to the organization's administrator. If an administrator was not listed on the account, we emailed the primary invoice contact. If you did not receive this email, please contact your organization administrator or primary invoice contact for next steps. You can use the KB article, linked here, to determine who your Organization Administrator is. Please access this KB article, linked here, to determine who your Primary Invoice Contact is.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. We have built this step-by-step toolkit in the event you and your organization determine that you need to notify your constituents. The following toolkit should be used to ensure that you are taking the right steps in communicating efficiently and effectively with your constituents.

Step 1: Identify the laws governing your jurisdiction and sector, as well as where your constituents reside.

Breach notification laws govern how an organization that owns or controls personal data notifies its constituents about a data breach involving their information. Most jurisdictions (states, territories, provinces, countries, etc.) have their own breach notification law. Not only should you review the law of the jurisdictions in which your organization operates but also the jurisdictions in which your constituents reside. Some jurisdictions' laws make you notify residents of a data breach even if you don't do business there. There are some sector-specific laws too—laws like HIPAA and FERPA—that cover protected health information and student records, respectively. To learn more about laws commonly applicable to our customers, please refer to our *Data Breach Reporting Guide*, which is linked here.

Step 2: Determine the types of data you collect.

It's important to understand what kind of data your organization collects to determine your notification requirements. **A copy of your backup file was part of this incident so look at the data fields you use in your Blackbaud Solution that was involved in this incident. Remember, though, that the file the cybercriminal removed a copy of did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted.**

Step 3: Determine your notification requirements.

Look at the laws identified in Step 1 and ask yourselves:

(1) Is the data that was accessible in my backup file the kind of data covered by the law?

Take the types of data you determined in Step 2 and compare them to the definition of personal data in your law that creates a notification obligation. For example:

'My organization is in a US state whose law defines personal information as a constituent's name and one of the following: Social Security number, driver's license number, or payment card, health care information or biometric data, or financial account number in combination with a required security code or password that permits access to that account. None of those data types were present in my backup file or were present but were stored in encrypted fields. Therefore, I don't need to notify affected constituents under this state law.'
'My organization is a covered entity or business associate under HIPAA, but the data in my backup file isn't classified as protected heath information. Therefore, I don't need to notify affected constituents under HIPAA.'

(2) If yes, does this law require notification based on a risk of harm?

Almost all of the world's data breach notification laws require notification only for breaches that pose a risk to individuals. The reason for this is simple—the purpose behind requiring notification is to ensure that affected individuals can take precautions to prevent harm to themselves, such as cancelling credit cards or obtaining identity theft protection. Determine if the law applicable to you only requires notification for breaches that are likely to result in risk ("high risk," "material risk," "real risk of significant harm" are also frequently used thresholds). A security incident poses a risk to your constituents if it's likely to harm your constituents. The focus of these laws is primarily damage in the form of identity theft and financial harm, but they can also include threats of physical or reputational harm.

(3) If yes, do I believe that Blackbaud's security incident will likely harm my constituents?

To assess the risk posed by a security incident, we consider both the severity of the consequences to an individual and the likelihood this impact will occur. I.e. 'how can this data be misused and is it likely to happen?'

Assess what kind of harm is possible considering factors like the types and sensitivity of data (*e.g. contact data vs. medical data*), the nature of the harm (*e.g. financial vs. reputational*), and other characteristics that may make data disclosure more or less harmful. Next, assess whether or not those consequences are likely. Remember that organizations must focus on *real* risk, not the risk that has a remote possibility of happening. We do not believe this incident poses any risk to your constituents because, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

Step 4: Notify constituents and required third parties, if you've determined it's required.

If you determine that notification is required, review the specifics in the law applicable to your organization. The law will specify when and in what manner constituents should be notified, such as by postal mail or email. We have provided you with template notification letters at the end of this Toolkit that you can use to notify your constituents of this security incident. Organizations may take advantage of substitute notice—an option included in some laws—but only if you don't have sufficient contact information or notification would require

disproportionate effort, as defined in that law (e.g. having to notify a lot of individuals in one place or if notification will cost over a certain amount). Substitute notice usually requires email notice and/or a conspicuous notice on your website, and sometimes even notification to media outlets. Some laws may also require you to notify third parties, like supervisory authorities, US state attorneys general, or credit reporting agencies. You can read more about these requirements in the laws or our *Data Breach Reporting Guide*, which is linked here.

You can also watch this on-demand webinar to hear details on determining your organization's legal obligations to notify constituents. Please click this link to access that webinar.

Notification Letter Template

[Use this form letter if you've determined that you are required to notify constituents]

[Date], 2020

[Insert mailing address (if law requires notification by postal mail) or email address (if law permits notification by email)]

RE: Notice of Data Breach

Dear [Name],

We are writing to let you know about a data security incident that may have involved your personal information. [Organization Name] takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened
We were recently notified by one of our third-party service providers of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, the service provider's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

What Information Was Involved
It's important to note that the cybercriminal did not access your credit card information, bank account information, or social security number. However, we have determined that the file removed may have contained your [company to list information contained in the subset of data removed by the cybercriminal – example: your contact information, demographic information, and a history of your relationship with our organization, such as donation dates and amounts.]

Because protecting customers' data is their top priority, our third-party service provider paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.
Based on the nature of the incident, their research, and third party (including law enforcement) investigation, we have 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.

What We Are Doing
We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, our third-party service provider has already implemented several changes that will protect your data from any subsequent incidents.

First, the provider's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. We have confirmed through testing by multiple third parties, including the appropriate platform vendors, that our fix withstands all known attack tactics. Additionally, they are accelerating our efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do
As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. [Insert contact information required by applicable law, such as for national credit reporting agencies, your country's or province's data protection regulator or trade commission, and/or your state's attorney general].

For More Information
We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact [Organization Contact Name] at [Organization Contact Phone Number] or [Organization Contact Email].

Sincerely,
[Name]
[Title]
[Organization]
[Address]

Notification Letter Template under the GDPR

[Use this form letter if you've determined that you are required to notify constituents who reside in the UK or EU]

[DATE], 2020
Via E-Mail
[Constituent Contact Name]
[Contact Title]

Re: *Notification of a personal data breach affecting constituents of [Organisation Name]*

Dear [Mr./Ms.] [Constituent Contact Name]:

[Insert Organisation Name] is notifying you of a data breach which may have affected your personal data. To the extent that the data breach affects constituents residing in the UK or EU, please accept this letter as a notification pursuant to Article 33(2) of the General Data Protection Regulation ("GDPR").

What Happened
We were recently notified by one of our third-party service providers of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, the service provider's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on 7 February 2020 and could have been in there intermittently until 20 May 2020.

What Information Was Involved
It's important to note that the cybercriminal did not access your credit card information, bank account information, or social security number. However, we have determined that the file removed may have contained your [organisation to list information contained in the subset of data removed by the cybercriminal – example: your contact information, demographic information, and a history of your relationship with our organization, such as donation dates and amounts.]

Because protecting customers' data is their top priority, our third-party service provider paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. **Based on the nature of the incident, their research, and third party (including law enforcement) investigation, we have 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.**

What We Are Doing
We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, the third-party service provider has already implemented several changes that will protect your data from any subsequent incidents.

First, the provider's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that our fix withstands all known attack tactics. Additionally, they are accelerating our efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do
As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. [Insert contact information

required by applicable law, such as for national credit reporting agencies, your country's or province's data protection regulator or trade commission, and/or your state's attorney general].

For More Information
We sincerely apologise for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact [Organisation Contact Name] at [Organisation Contact Phone Number] or [Organisation Contact Email].

Sincerely,
[Name]
[Title]
[Organisation]
[Address]

Website Notification Template

[Post this notice on your website if you've determined that you are required to notify constituents and are taking advantage of substitute notice. Remember that you can only use substitute notice if your law allows it and you don't have sufficient contact information or notification would require disproportionate effort, as defined in that law (e.g. having to notify a lot of individuals in one place or if notification will cost over a certain amount). If you are notifying constituents directly by postal mail or email, you do not need to use this template, unless your law requires you to post the notice on your website.]

Notice of Data Breach

What Happened
We were recently notified by one of our third-party service providers of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, the service provider's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

What Information Was Involved
It's important to note that the cybercriminal did not access your credit card information, bank account information, or social security number. However, we have determined that the file removed may have contained your [company to list information contained in the subset of data removed by the cybercriminal – example: your contact information, demographic information, and a history of your relationship with our organization, such as donation dates and amounts.]

Because protecting customers' data is their top priority, our third-party service provider paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, their research, and third party (including law enforcement) investigation, we have 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.

What We Are Doing
We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, our third-party service provider has already implemented several changes that will protect your data from any subsequent incidents.

First, the provider's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. We have confirmed through testing by multiple third parties, including the appropriate platform vendors, that our fix withstands all known attack tactics. Additionally, they are accelerating our efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do
As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. [Insert contact information required by applicable law, such as for national credit reporting agencies, your country's or province's data protection regulator or trade commission, and/or your state's attorney general].

For More Information
We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact [Organization Contact Name] at [Organization Contact Phone Number] or [Organization Contact Email].