17319

July 25, 2020

Mr./Mrs.
address

Dear,

We are writing to let you know about a data security incident with Blackbaud, a third-party provider, that may have involved your personal information. Many colleges and non-profits including Mercy College use Blackbaud for engagement and fundraising data services. Mercy College met with Blackbaud on July 20, 2020 to review details regarding a security incident involving their systems.

Mercy College takes the protection and proper use of your information very seriously. We are therefore contacting you as a precautionary measure to explain the incident and provide you with steps you can take to protect your personal information.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also place a security freeze on your credit reports, free of charge. **Mercy intends to provide these services on your behalf, and we will be following up with you about this further in the coming week.** A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, Mercy will be providing you with information about how we will assist in obtaining this service, or you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests

made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

We sincerely apologize for this incident and regret any inconvenience it may cause you. We deeply value your relationship with Mercy College. Should you have further questions, please contact Bernadette Wade at bwade@mercy.edu or Camille Shelley at cshelley@mercy.edu.

Sincerely,

Bernadette Wade
Chief Advancement Officer
bwade@mercy.edu
914-357-3883

Camille Shelley
Chief Information Officer
cshelley@mercy.edu
914-674-7131

Blackbaud Security Incident Resources for Involved Customers

Summary Webinars Frequently asked questions Toolkits Contact us

This page is for use by organizations who were notified on July 16, 2020 of a security incident at Blackbaud. The reason you have access to this page is because your organization needed to be notified. Please read the information below and then click the tabs for details on webinars, frequently asked questions, a notification toolkit, and contact information.

What happened

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. Like many in our industry, Blackbaud encounters millions of attacks each month, and our expert Cybersecurity team successfully defends against those attacks while constantly studying the landscape to stay ahead of this sophisticated criminal industry. We wanted to notify our customers and other stakeholders about a particular security incident that recently occurred.

Summary of Incident

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 is 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. The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.

More about Blackbaud's Cybersecurity Practices and Next Steps Following this Incident

Over the last five years, we have built a substantial cybersecurity practice with a dedicated team of professionals. Independent reviewers have evaluated our program and determined that it exceeds benchmarks for both the financial and technology sectors. We follow industry-standard best practices, conduct ongoing risk assessments, aggressively test the security of our solutions, and continually assess our infrastructure. We are also a member of various Cyber Security thought leadership organizations, including: The Cloud Security Alliance and Financial Services Information Sharing and Analysis Center (FS-ISAC), where we team up with other experts to share best practices and tactical threat information for the Cyber Security community. We believe the strength of our cybersecurity practice and advance planning is the reason we were able to shut down this sophisticated ransomware attack. We have already implemented changes to prevent this specific issue from happening again. You can review more details on our security, risk, compliance and privacy programs here.

What this Means for Your Organization

We notified organizations involved in this incident on July 16, 2020 by sending an email to your organization's administrator, unless one wasn't listed on your account. In that case, we emailed the primary invoice contact. This email specifically outlined any solution(s) of yours that were part of this incident. If you received this email from Blackbaud about this incident, please use the resources below to guide your organization's next steps.

- If you were given this link by a Blackbaud representative but did not receive the email, your organization was part of this incident. The fastest way to get information for your organization is to contact your organization administrator or primary invoice contact—they will have details. 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.

Your Organization's Next Steps

Most of our customers will not have legal or regulatory need to notify their constituents because of the types of data that may have been exposed and because 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. However, for any who determine they should notify their constituents, we have provided this toolkit with templates to support you. And your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements.

From: Joel Carter <joel.carter@blackbaud.com>
Sent: Thursday, July 16, 2020 11:10 AM
To: McGrath Rothenberg, Alexis <arothenberg@mercy.edu>
Subject: [EXT]: Notification of Security Incident

Dear Alexis,

Please see a personalized note below for your organization from our Chief Information Officer. Thank you.

Dear Alexis,

We are writing to notify you about a particular security incident that recently occurred. Please review this email for a personalized link, next steps and resources created for your organization specifically.

What Happened

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 attempted 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. 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.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud NetCommunity, Blackbaud Raiser's Edge NXT, and ResearchPoint backup was part of this incident. Again, 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. None of your data was lost or corrupted as a result of this incident.

And again, 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.

We have created a resource page for you at www.blackbaud.com/incidentresources that features a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars (hosted by Rich Friedberg, Blackbaud's Chief Information Security Officer and Cameron Stoll, our Head of Privacy), information about our future plans, and other resources.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. 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 your toolkit to make it easier.

To ensure all your questions are answered as quickly as possible, we encourage you to first review the resources we provided at the link above. If you still have questions after reviewing these resources, we are here to help. 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

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.

Sincerely,

Todd Lant
Chief Information Officer

Please add joel.carter@blackbaud.com to your address book or safe senders list.

Manage your subscription preferences.

What happened?

We discovered and stopped a ransomware attack. In a ransomware attack, cyber criminals attempt to disrupt a 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.

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.

The data set the cybercriminal was exposed to did not contain any credit card information. The cybercriminal did not access bank account information or social security numbers because they were encrypted.

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 situation. We have already implemented changes to prevent this specific issue from happening again.

When did you learn of this incident?

In May (2020).

Which products/solutions were involved in this incident?

This incident was limited to a subset of our self-hosted (or co-located) environment. No entire product line was part of this incident. This incident did not reach solutions to the public cloud environment (Microsoft Azure, Amazon Web Services), nor did it reach the majority of our self-hosted environment. Customers whose products/solutions were part of this incident have been notified.

Did you pay the cybercriminal to contain the information they had?

Yes, we went to all appropriate measures to protect our customers' data, which was our top priority in that situation. We have no reason to believe that any data was or will be made available publicly. As a matter of fact, we did not pay them until we received

assurance that they destroyed the data. And as a precautionary measure, we have hired outside experts to monitor the dark web and they have found no evidence that any information was ever released.

How can you be sure the information the cybercriminal was exposed to is contained and wasn't sold online?

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. Their motivation was to disrupt our business by encrypting customer files in our datacenters, which we were able to prevent. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

Are you able to provide me with a copy of the backup file that was removed by the cybercriminal?

All unencrypted data fields in your backup files for the solutions we included in our email to you were part of this incident. To view the fields your organization uses, you can access your production database—the data fields will be the same as in your backup file. You can exclude credit card information, which was stored elsewhere, and data stored in encrypted fields such as bank account information, social security numbers, and usernames and passwords stored within your database. For a complete list of encrypted fields that were not accessible, please search https://kb.blackbaud.com for a list of encrypted fields for your specific Blackbaud solution ("What fields are encrypted in the database").

How do I assess my notification obligations?

- First, determine which notification laws apply to your organization. We have provided a toolkit containing a written guide and access to a webinar discussing these laws. This analysis is important because most laws require notification only if the data accessed was of a certain type that regularly leads to identity theft or fraud, like financial information or social security numbers. If the kind of data in your backup files isn't one of the types stated in the definition of personal data that triggers notification, then you do not need to notify anyone. Finally, under most breach notification laws, if harm (or even significant harm, as under the GDPR) to affected constituents isn't likely, then you aren't required to notify those individuals. Again, based on our 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 so we do not believe that harm is likely to result to your constituents.
- Second, determine the types of data your organization stores in its impacted backup file and compare it to any notification requirements that you determined in the step above. To do this, assess the fields your organization uses by viewing your production database—the data fields will be the same. You can exclude

credit card information, which was stored elsewhere, and data stored in encrypted fields such as bank account information, social security numbers, and usernames and passwords stored within your database. For a complete list of encrypted fields that were not accessible, please search https://kb.blackbaud.com for a list of encrypted fields for your specific Blackbaud solution ("What fields are encrypted in the database").

How do I determine which of my constituents were part of this incident from my database?

- The constituents listed in the backup files for the solutions we included in our email to you were part of this incident. Your backup files may have been accessed by the cybercriminal between February 7 and May 20. If you are attempting to determine which records may have been in your database during this period, most our solutions will allow you to query for any records added before a specified date. For instructions on how to do that, please search https://kb.blackbaud.com (e.g., "How to query on constituents added within a specific date range") to determine what was present in your backup files in that time frame.

What assistance are you providing to help me communicate with my organization's constituents?

- Most of our customers will not have legal or regulatory need to notify their constituents because of the types of data that may have been exposed and because 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. However, for any who determine they should notify their constituents, we have provided a toolkit with templates to support you. And your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements.

Has your platform been audited/pen tested?

- Yes, our platform was audited/pen tested by three external entities over the last several years. Independent reviewers who have studied our program have determined that it exceeds benchmarks for both the financial and technology sectors.

How will this incident affect our/your work?

- We will maintain our commitments to you. We have resources that are focused solely on the implementing new measures to protect your data, but we also have the resources to continue providing you with the reliability and stability you expect.

Why didn't you contact us in May?

- When an attack this sophisticated is discovered, there is a lot of work to do. First, we prioritized the work we know you would expect: fending off the cybercriminal's attempt to encrypt our customer files, preventing them from blocking our system access, and expelling them from our system. Prioritizing this first allowed us to successfully defend against this attack. Next, we began a thorough investigation. This involved partnering with independent forensics experts and law enforcement to investigate the cybercriminal, doing extensive research and analysis on the files behalf of all our customers to determine if any information had been corrupted or otherwise impacted, producing tools and resources for our customers and deploying measures to ensure this doesn't happen again. We went as fast as we could, but all of this takes time. As we've said, we are committed to our partnership with our customers. Part of that commitment includes making sure we knew everything that happened, so we could accurately report those details to our customers.

I want to talk to someone about this incident. Who can I talk to?

- If you still have questions after reviewing the resources we've provided, we're here to help. 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
    - **Asia Pacific Region:** Please email jenny.bloch@blackbaud.com