

August 25, 2020

State of New Hampshire
Office of Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Blackbaud Security Breach Affecting Crisis Center of Central New Hampshire Donors

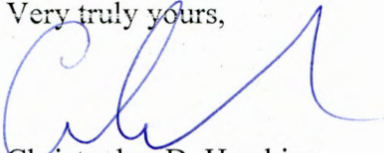
To Whom it May Concern:

This office represents the Crisis Center of Central New Hampshire (“CCCNH”). CCCNH utilizes a secure platform called Blackbaud to maintain donor data. On July 16th, CCCNH received notice that in May of 2020, Blackbaud experienced a ransomware attack that affected. Blackbaud informed CCCNH that the attack did not affect the donor’s credit card information, social security numbers, or bank account information. It appears the only information obtained was the donor’s names, addresses, phone numbers, and email accounts. A copy of the notice received from Blackbaud is attached as Exhibit A.

Pursuant to RSA 395-C:20, I(b), please be advised that the CCCNH notified the affected individuals by email on August 13, 2020, and by regular mail on August 14, 2020. A sample of the notice is attached as Exhibit B. Approximately 2,000 people in New Hampshire were affected by this issue. Pursuant to RSA 395-C:20, VI(a), notice is being provided to Experian, Equifax, and TransUnion by means of this letter.

If you have any questions regarding this matter, please do not hesitate to contact me.

Very truly yours,



Christopher D. Hawkins

CDH/klr

Enclosures

cc: Debbie Johnson, CCCNH
Experian (databreachhelp@experiandirect.com)
TransUnion (555 West Adams St., Chicago, IL 60661)
Equifax (1550 Peachtree St., Atlanta, GA 30309)

Exhibit A

blackbaud®

Dear [REDACTED],

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

Dear [REDACTED],

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 eTapestry 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](http://www.blackbaud.com/incidentresources) 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

blackbaud

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").

Exhibit B



CRISIS CENTER *of* Central New Hampshire

Dear CCCNH Community ,

We are writing to share information about a data security incident that occurred at Blackbaud earlier this year. Blackbaud is a cloud-based software company used by K-12 schools, nonprofit organizations, and foundations. As a member of our community, we are sending this notice as a precaution to provide you with more information about what happened. CCCNH values our community and wants to be fully transparent and open about the cyber attack at Blackbaud.

Please note that this incident *did not* affect any financial account information, credit or debit card information or Social Security numbers. Although CCCNH does not store these types of sensitive personal information, we take the privacy and protection of your information very seriously.

What Happened

We were recently notified by Blackbaud that they were the victim of a security incident involving an attempt to deploy ransomware. While Blackbaud, in conjunction with independent forensics experts and law enforcement, was able to successfully prevent the malicious files from executing, they believe the unauthorized third party responsible for the incident may have been able to access certain files, including a backup file belonging to CCCNH containing information on members of the CCCNH community.

While the information stored in the backup file varies by individual, it may include first and last name, address, email address, and phone numbers. **As outlined above, the file *did not* contain any information regarding credit or debit card numbers, financial account information, or Social Security numbers.**

Because protecting customers' data is their top priority, Blackbaud 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.

Next Steps

Although we maintain detailed data protection and privacy policies with all our vendors, we are continuing to review and enhance our security procedures and measures to help prevent this type of incident from recurring in the future.

According to the information that we received, Blackbaud engaged a leading cybersecurity firm to support its investigation and response and has coordinated with law enforcement following this incident. They have implemented additional security controls and system hardening procedures to better protect the data they maintain.

Although we are not aware of misuse of any information arising out of the incident, we are reaching out to those whose information was contained in the aforementioned backup file. As a best practice, we recommend you remain vigilant and cautious of any unexpected communications purporting to come from CCCNH. If you ever have questions about the legitimacy of any communications you receive that appear to come from CCCNH, particularly those that relate to any sort of payment or financial information, we recommend contacting us directly at [REDACTED] to confirm that the email was sent from CCCNH.

We value our relationship with you and are committed to protecting the security and privacy of the information you provide to us. We sincerely regret that this incident occurred and 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 us at [REDACTED].

Sincerely,



Jennifer Pierson
Executive Director
