17737

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 Financial Edge NXT, 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.

If it has not already happened, someone from our team will be reaching out to your organization directly in the next 24 hours. In the meantime, we encourage you to review the resources we provided at the link above. If you have additional questions after reviewing these resources and after speaking to the team member who reaches out to you today, you can 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

Dear [redacted]

Thank you for your service. We are supplementing our prior notice to include additional information. As you are aware, one of our vendors, Blackbaud, had a security incident, which may have resulted in a breach of your personal information, specifically your credit card number.

On July 16, 2020, the New Covenant Trust Company, NA was notified by our service provider, Blackbaud, about a security incident that took place in May 2020, whereby an unauthorized party used malware to gain access to and download files from Blackbaud's servers that included New Covenant Trust Company data.

Although Blackbaud informed us that credit card information was not compromised, after conducting our own internal investigation of every invoice scanned, we determined that the affected data included scanned invoices that contained a credit card number of yours from a statement submitted as part of a reimbursement request.

We are not aware of any misuse of your information; however, out of an abundance of caution, we are providing you with this notification.

There are important steps that you can take to reduce the likelihood of identity theft or fraud:

The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should also monitor any suspicious activity associated with your financial accounts. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-ID-THEFT (877-438-4338) or visit the FTC's website at http://www.ftc.gov/bcp/edu/microsites/idtheft/. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency or the Massachusetts Attorney General.

CREDIT MONITORING INSTRUCTIONS

Please know that protecting your personal information is a matter we take very seriously, and we and Blackbaud have taken actions designed to prevent unauthorized access. Blackbaud stated that it paid a requested ransom to the unauthorized party, and the unauthorized party represented that it deleted the data taken from Blackbaud.

As previously explained, to help protect your identity, we are offering complimentary credit monitoring services. This service helps detect possible misuse of your personal

information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

Please contact Greg Rousos or Angela Duffy if you would be interested in utilizing this service and we will cover the cost.

OBTAINING A POLICE REPORT

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.

PLACING A SECURITY FREEZE ON YOUR CREDIT REPORT

Consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. There is no fee to place a security freeze on your credit report. 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.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below:

Experian	**Equifax**	**TransUnion**
Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016

To request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
- 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;
- If you are not a victim of identity theft, include payment by check, money order, or credit card Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

You can also place security freezes online by visiting the following websites:

- **Experian:** https://www.experian.com/freeze/center.html
- **Equifax:** https://www.equifax.com/personal/credit-report-services/
- **TransUnion:** https://www.transunion.com/credit-freeze

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (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 or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days 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 send a written request to each of the three credit bureaus by mail and include 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 three (3) business days after receiving your request to remove the security freeze.

QUESTIONS?

We sincerely regret that this incident occurred. If you have any questions, please feel free to contact us at 502.569.5857 or email me at angela.duffy@presbyterianfoundation.org. As always, we appreciate your service and commitment to New Covenant Trust Company, NA.