WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

September 14, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Privileged and Confidential
Via Email Only

Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antirust
1050 E. Interstate Avenue, Ste. 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: Data Security Incident

Dear Attorney General Stenehjem:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Lakes & Prairies Community Action Partnership ("CAPLP"), located at 715 11th St. N., Ste. 402, Moorhead, MN 56560, with respect to a data security incident involving Blackbaud, Inc. ("Blackbaud"), a third-party provider used by CAPLP to process and store information, as described in more detail below.

1. Nature of the security Incident.

CAPLP is a nonprofit whose mission is to eliminate poverty, empower families, and engage communities. In July 2020, as your Office may already be aware, Blackbaud notified hundreds of nonprofits, including CAPLP, that Blackbaud experienced a ransomware incident in May 2020 which may have resulted in the exposure of personal information maintained by nonprofits on the Blackbaud platform. CAPLP was first notified of this incident by Blackbaud on July 16, 2020 that Blackbaud experienced a cybersecurity incident ("Blackbaud Incident") which resulted in the exposure of personal information maintained by hundreds of non-profit and educational institutions on multiple Blackbaud platforms. (A copy of Blackbaud's notice of the Incident is attached.) Blackbaud is a cloud computing provider that is used by CAPLP and many other institutions to organize and store information related to members of their community. After an initial investigation, CAPLP discovered the Blackbaud platform they use called *Financial Edge*, contained the name, home address, email address, and date of birth of CAPLP employees. According to communication from Blackbaud, Blackbaud did not encrypt this platform, containing the backup dataset of CAPLP data. However, Blackbaud has conveyed to CAPLP that sensitive text fields such as the Social Security number field are encrypted. While CAPLP does utilize *Financial Edge* to store Social Security numbers, Blackbaud has advised that this field is encrypted and therefore this information was not viewed by the threat actor during the cyber security incident. At this time, based on the information CAPLP received from Blackbaud, CAPLP has no reason to believe that any personal information of any members of the CAPLP community has been or will be misused as a result of this incident.

2. Number of North Dakota residents affected.

A total of three hundred twenty-five (325) North Dakota residents may have been potentially affected by this incident. While CAPLP is not aware of any misuse of employee information, CAPLP is notifying these individuals of the Blackbaud Incident out of an abundance of caution since the information included individual's dates of birth which constitutes protected information under North Dakota's privacy law. A notification letter to these individuals was mailed on September 14, 2020 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

CAPLP takes the privacy and security of their information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Upon discovery of the incident, CAPLP immediately informed Wilson Elser Moskowitz Edelman & Dicker LLP, and began identifying the individuals contained within the *Financial Edge* platform in preparation for notice. CPALP has also requested Blackbaud to explain the steps it has taken to mitigate the risk of a similar attack. Blackbaud has stated that 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 their fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

4. Contact information.

CAPLP remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.

[redacted].

From: [redacted]
Sent:
To:
Subject: FW: Notification of Security Incident

[redacted]

[redacted]

[redacted]

From: Customer Success <customersuccess@blackbaud.com>
Sent: Thursday, July 16, 2020 10:46 AM
To: [redacted]
Subject: Notification of Security Incident

[redacted]

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

[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 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

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>> <<State>><<Zip>> <<Date>>

Dear <<First Name>><<Last Name>>:

We are writing to inform you of a data security incident involving Blackbaud, Inc. ("Blackbaud"). Lakes and Prairies Community Action Partnership, Inc. ("Lakes and Prairies") takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

Blackbaud is a cloud computing provider that is used by Lakes and Prairies and many other charitable organizations to organize and store information related to members of our community. In July 2020, as you may already be aware, Blackbaud notified hundreds of educational institutions, including Lakes and Prairies, that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and charitable organizations on the Blackbaud platform. Lakes and Prairies was first notified of this incident by Blackbaud July 16, 2020.

At this time, based on the information we have received from Blackbaud, we have no reason to believe that any of your personal information has been misused as a result of this incident. However, for purposes of full disclosure, we feel it is important to inform you that some of your personal information may have been viewed by unauthorized individuals as a result of this incident, including your date of birth as discussed below.

Specifically, Lakes and Prairies utilized the Blackbaud platform known as *Financial Edge*. We feel it is important to inform you that we used the *Financial Edge* platform to store the following unencrypted information which we believe may have been exposed as a result of this incident: your name, home address, and your date of birth.

Lakes and Prairies also used *Financial Edge* to store your Social Security number. However, as confirmed by Blackbaud, all Social Security numbers were stored in an encrypted format for security purposes. Thus, according to Blackbaud, no Social Security numbers were exposed to any unauthorized parties as a result of this incident.

Lakes and Prairies is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. As always, we recommend that you continue to join us in remaining vigilant to protect your information.

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have any questions, please do not hesitate to call 218.512.1508 Monday through Friday 9 AM CST to 4 pm CST.

Sincerely,

Lori Schwartz, M.S., CCAP, NCRT
Executive Director
218.512.1506 | www.caplp.org
715 11th St N. Suite 402 | Moorhead, MN 56560

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri, North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.