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

Eric R. Benson
(914) 872-7728 (direct)
Eric.Benson@wilsonelser.com

January 29, 2021

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notification of Data Security Incident Pursuant to 10 M.R.S. § 1348(5)

To Whom It May Concern:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents The Opportunity Alliance ("TOA") of South Portland, Maine, with respect to a data security incident involving TOA's cloud computing provider, Blackbaud, Inc. ("Blackbaud").

1. Nature of the Security Incident

Blackbaud is a cloud computing provider that The Opportunity Alliance uses to maintain and store information related to The Opportunity Alliance community, including TOA clients and TOA employees. Blackbaud has notified numerous organizations, including The Opportunity Alliance, that Blackbaud experienced a cybersecurity incident during the spring of 2020 (hereinafter, the "Incident") which resulted in the exposure of personal information maintained via Blackbuad's customers on Blackbaud's platforms.

Based on the information provided by Blackbaud, The Opportunity Alliance has discovered that the Incident resulted in the exposure of personal information and/or protected health information pertaining to current and former clients and employees of The Opportunity Alliance. The elements of personal information that were exposed varied per individual, and included information such as client names, addresses, dates of birth, and social security numbers. Additionally, in some instances, The Opportunity Alliance discovered that the incident may have resulted in exposure of certain medical information pertaining to clients such as medical service information, MaineCare ID, treatment and/or prescription information, diagnostic information, and health insurance information.

2. Number of Maine Residents Affected

Based on the information provided by Blackbaud, and with the assistance of a third-party cybersecurity forensics vendor, The Opportunity Alliance has discovered that the incident resulted in the exposure of protected health information and/or personally identifiable information of a population of at least two

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

thousand three hundred and thirty seven (2,337) residents of the state of Maine (hereinafter, the Affected Population).

Of the Affected Population, one thousand eight hundred and five (1,805) individuals are TOA clients. In accordance with the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, and in accordance with Maine's Notice of Risk to Personal Data Act (10 M.R.S.A. §§1346-1350-B), each of these clients were mailed an incident notification letter on or about Monday January 25, 2021. Please see **Exhibit A** for a sample copy of the notification letter that TOA sent to affected clients.

The remaining five hundred and thirty-two (532) affected individuals are current or past employees of TOA whose names and social security numbers were exposed as a result of the Incident. In accordance with 10 M.R.S.A. §§1346-1350-B, TOA will notify this population of employees via mail on February 1, 2021. Please see **Exhibit B** for a sample copy of the notification letter that TOA will send to affected employees.

3. Steps Taken

After receiving initial notification of the Incident on July 16, 2020, TOA quickly launched an internal investigation and demanded additional information from Blackbaud. The limited information that Blackbaud provided TOA in Blackbaud's July 2020 notice did not enable TOA to sufficiently determine which unencrypted data was potentially compromised as a result of the ransomware incident.

Please note that Blackbaud has repeatedly failed to provide TOA with timely responses to TOA's requests for information (both formal and informal), and, as such, TOA has taken independent action to assess the scope of this breach without timely and critical assistance from Blackbaud. Specifically, TOA hired a third-party cybersecurity forensics firm to assist TOA in accounting for what information maintained by TOA via Blackbaud was impacted by the Incident.

Nonetheless, Blackbaud has informed The Opportunity Alliance that Blackbaud is taking action to prevent a similar event from occurring in the future through the performance of regular penetration testing and the deployment of additional security controls. At all times, in both its customer contracts and Privacy Policy, Blackbaud has represented that it maintains administrative, physical and technical safeguards designed to protect against threats to the security and unauthorized access of TOA's data.

TOA remains dedicated to protecting the sensitive information within 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 AND DICKER LLP

Anjali C. Das
Equity Partner

Eric R. Benson
Associate Attorney

Cc: Experian: businessrecordsvictimassistance@experian.com
Equifax: security.dataadministration@equifax.com
TransUnion: FVAD@Transunion.com

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

EXHIBIT A

<<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 our third-party cloud computing vendor, Blackbaud, Inc. ("Blackbaud"). The Opportunity Alliance takes the security of your 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.

What Happened

Blackbaud is a cloud computing provider that The Opportunity Alliance uses to maintain and store information related to our organization and members of our community. In July 2020, Blackbaud notified hundreds of organizations, including The Opportunity Alliance, that Blackbaud experienced a cybersecurity incident in May 2020 which resulted in the exposure of personal information maintained via organizations on Blackbaud's platforms. After receiving notification of the incident, The Opportunity Alliance launched an internal investigation and demanded additional information from Blackbaud to determine exactly what happened and how the incident may have impacted our community.

What Information Was Involved

At this time, based on the information we have received from Blackbaud, we have no reason to believe that any personal information of past or current clients of The Opportunity Alliance has been or will be misused as a result of this incident. However, for purposes of full disclosure and based on information we have received from Blackbaud, we feel it is important to inform you that elements of your personal information may have been exposed as a result of this incident. These elements include, but may not be limited to: your name, your address, your date of birth, and your social security number. Additionally, The Opportunity Alliance discovered that the incident may have resulted in exposure of certain medical information related to you, including but potentially not limited to: your medical record number, medical service information, MaineCare ID, treatment and/or prescription information, diagnostic information, and health insurance information.

What We Are Doing

We continue to closely monitor the situation and we are working with cybersecurity experts to determine the actions to take in response. Blackbaud has informed us that they are taking action to prevent a similar event from occurring in the future through the performance of regular penetration testing and the deployment of additional security controls.

For More Information

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. As always, we recommend that you continue to join us in remaining vigilant to protect your information. Steps that you may consider taking to protect your information are included on the following page. If you have any questions about this matter, please do not hesitate to call our compliance help line at 207-200-2623 or toll free at 800-698-4959 Monday – Friday, 8am to 5pm.

Sincerely,

Joseph R. Everett

President & CEO
The Opportunity Alliance

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 Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina 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

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

EXHIBIT B

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>> <<Date>>

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

We are writing to inform you of a data security incident involving our third-party cloud computing vendor, Blackbaud, Inc. ("Blackbaud"). The Opportunity Alliance takes the security of your 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.

What Happened

Blackbaud is a cloud computing provider that The Opportunity Alliance uses to maintain and store information related to our organization and members of our community. In July 2020, Blackbaud notified hundreds of organizations, including The Opportunity Alliance, that Blackbaud experienced a cybersecurity incident in May 2020 which resulted in the exposure of personal information maintained via organizations on Blackbaud's platforms. After receiving notification of the incident, The Opportunity Alliance launched an internal investigation and demanded additional information from Blackbaud to determine exactly what happened and how the incident may have impacted our community.

What Information Was Involved

At this time, based on the information we have received from Blackbaud, we have no reason to believe that any personal information of past or current employees of The Opportunity Alliance has been or will be misused as a result of this incident. However, for purposes of full disclosure and based on information we have received from Blackbaud, we feel it is important to inform you that elements of your personal information may have been exposed as a result of this incident. These elements include, but may not be limited to: your name and social security number.

What We Are Doing

We continue to closely monitor the situation and we are working with cybersecurity experts to determine the actions to take in response. Blackbaud has informed us that they are taking action to prevent a similar event from occurring in the future through the performance of regular penetration testing and the deployment of additional security controls.

For More Information

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. As always, we recommend that you continue to join us in remaining vigilant to protect your information. Steps that you may consider taking to protect your information are included on the following page. If you have any questions about this matter, please do not hesitate to call (207) 200-2623 or toll free at (800) 698-4959, Monday – Friday, 8am to 5pm.

Sincerely,

Joseph R. Everett

President & CEO
The Opportunity Alliance

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 Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Maryland and North Carolina 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

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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