WINSTON & STRAWN LLP North America Europe Asia

35 W. Wacker Drive
Chicago, IL 60601
T +1 312 558 5600
F +1 312 558 5700

SHERYL FALK
Partner
(713) 651-2615
SFalk@winston.com

VIA EMAIL

October 12, 2020

Bob Ferguson, Attorney General
SecurityBreach@atg.wa.gov.

Re: Notice of Blackbaud, Inc. Privacy Incident

Dear Attorney General Ferguson:

Winston & Strawn LLP ("Winston") represents ZERO – The End of Prostate Cancer ("ZERO") with respect to the Blackbaud, Inc. ("Blackbaud") privacy incident that is the subject of this letter. I am writing to inform this office of the incident pursuant to Washington law, as it potentially affected one thousand, one hundred thirty-nine (1139) Washington residents. ZERO is a 501(c)(3) philanthropic organization that utilized Blackbaud as one its third-party service providers.

On July 16, 2020, ZERO received notice from Blackbaud indicating that Blackbaud had discovered a ransomware attack on its systems in May 2020. According to Blackbaud, the attack was initiated sometime between February 7, 2020 and May 20, 2020. Blackbaud confirmed that, as a result of the incident, a copy of its back-up file that contained ZERO constituent personal information was removed from its system by the individual or group that initiated the ransomware attack. Upon learning of this incident, ZERO immediately launched an investigation to determine the scope and impact of the incident.

Following an extensive forensic investigation of its constituent records, on September 14, 2020, ZERO confirmed that the personal information of one thousand, one hundred thirty-nine (1139) Washington residents may have been affected by this incident. Such personal information may have included the Washington residents' first and last names, date of birth, contact information (e.g., address) and/or health-related information.

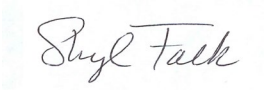
ZERO worked with legal counsel and Blackbaud to evaluate Blackbaud's response to the incident and the actions it has taken to best prevent against a similar incident occurring in the future. In particular, Blackbaud confirmed to ZERO that it worked with law enforcement to investigate the incident and that it is undertaking efforts to further strengthen its information

security infrastructure. ZERO is also taking steps to notify individuals who were potentially affected by the incident, including the Washington residents referenced in this letter, as required under applicable state notification laws. ZERO anticipates providing notification to all potentially affected individuals on or before October 14, 2020. A sample of the notification letter that ZERO is providing to potentially affected constituents is attached for your office's reference.

Please note that, by providing this information, ZERO expressly reserves all available rights, defenses, and privileges in connection with this incident. Furthermore, ZERO does not admit or concede any liability or wrongdoing, and expressly reserves its right to contest or challenge any findings or conclusions of any investigation by this office or any other office or agency with appropriate jurisdiction. Finally, this notice is not, and does not otherwise constitute, a waiver of ZERO's objection that Washington lacks personal jurisdiction with respect to the incident.

It is my hope that this information will satisfy this office's need for information related to this incident. However, if this office requires any additional details, please contact me by telephone at (713) 651-2615 or via email at SFalk@winston.com

Sincerely,



Sheryl A. Falk

Enclosure: Sample Notification Letter

ZERO
THE END OF PROSTATE CANCER

ZEROCANCER.ORG
Main Phone: 202-463-9455
Toll Free: 888-245-9455
Fax Phone: 571-257-8559

ZERO - The End of Prostate Cancer
515 King Street, Suite 420
Alexandria, VA 22314

[Recipient Name]
[Recipient Address]
[Recipient City, State, Zip Code]

[Date]

Dear [Recipient Name],

ZERO – The End of Prostate Cancer ("ZERO") takes the privacy and security of our constituent information seriously. We are writing to notify you of an incident experienced by Blackbaud, Inc. ("Blackbaud"), one of our third-party service providers, that may have impacted your personal information.

Blackbaud has confirmed that it is not aware of any misuse of the information affected by the incident. That stated, we are providing this notice out of an abundance of caution so that you may take action to protect your personal information, if you feel it is appropriate to do so.

What Happened? On July 16, 2020, ZERO received notice from Blackbaud that it discovered a ransomware attack on its systems in May 2020. According to Blackbaud, the attack was initiated sometime between February 7, 2020 and May 20, 2020. Blackbaud confirmed that, as a result of the incident, a copy of its back-up file that contained ZERO constituent personal information was removed from its system from the individual or group that initiated the ransomware attack. Upon learning of this incident, we immediately launched an investigation to determine the scope and impact of the incident.

What Information Was Involved? In connection with our investigation, on September 14, 2020, we confirmed that some of your personal information may have been affected by this incident. Out of an abundance of caution, we wanted to let you know that this may have included your first and last name, contact information (e.g., your address), your birth date and health-related information about you, including information that you provided to us regarding your medical status and treatments.

What Are We Doing. Information privacy and security are among our highest priorities. We have worked with our own legal counsel and Blackbaud to evaluate Blackbaud's response to the incident and the actions it has taken to best prevent against a similar incident occurring in the future. We have worked with our own legal counsel and Blackbaud to evaluate Blackbaud's response to the incident and the actions it has taken to best prevent against a similar incident occurring in the future. In particular, Blackbaud has communicated that it worked with law enforcement to investigate the incident and that it is undertaking efforts to further strengthen its information security infrastructure. We have also taken steps to notify individuals who were potentially affected by the incident, including you, as required under applicable state notification laws.

What Can You Do. While Blackbaud has indicated that it is not aware of any misuse of your personal information, we encourage you to remain vigilant and exercise caution in the event that anyone contacts you to request your personal information or monetary payments. We also encourage you to review the reverse entitled, "**Recommended Steps to Help Protect Your Information**."

How To Get More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact Jen Gomes, Director, Operations, at jen@zerocancer.org or 202-303-3105.

We sincerely regret any inconvenience this incident may cause you.

Sincerely,

Jamie Bearse
President and CEO
ZERO – The End of Prostate Cancer

Recommended Steps to Help Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place fraud alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Request a security freeze. By placing a security freeze, someone who fraudulently acquires your personal information will not be able to use that personal information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit, you may 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
- 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.)

4. Exercise your rights under the Fair Credit Reporting Act. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

5. Obtain additional information about the steps you can take to avoid identity theft. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse
Federal Trade Commission,
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TTY: 1-866-653-4261.