Schwabe
WILLIAMSON & WYATT®

September 11, 2020

Colin Folawn
Admitted in Washington and Oregon
T: 206-407-1500
cfolawn@schwabe.com

VIA E-MAIL

The Honorable Robert Watson Ferguson
Attorney General of Washington
Washington State Office of the Attorney General
800 Fifth Avenue, Suite 2000
Seattle, Washington 98104

RE: YouthCare: Blackbaud data incident
Our File No.: 125596-256665

Dear Mr. Attorney General:

My law firm represents YouthCare regarding a data incident involving its vendor, Blackbaud. Pursuant to RCW 19.255.010(7), we write to provide you with electronic notice of the data incident. To the best of our knowledge, 3,410 Washington consumers were affected by the incident.

A sample of the notification is attached. The types of personal information that were reasonably believed to have been at issue included name, address, date of birth, contact information, email address, gender, spouse's name, giving history, participation in YouthCare's efforts, demographic information, and other information that donors have provided to YouthCare. Blackbaud has indicated that the incident occurred from February 7, 2020, through May 20, 2020, affecting nonprofit organizations across the nation. Blackbaud's explanation can be found at: https://www.blackbaud.com/securityincident.

Blackbaud has informed YouthCare that its cyber security team, independent forensics experts, and law enforcement prevented the criminal from blocking system access and fully encrypting files and expelled the criminal from its system. Before being removed from the system, the criminal removed a copy of some data, but Blackbaud has told YouthCare that it paid a ransom in exchange for confirmation from the criminal that any data that was accessed and copied has been destroyed. We have been assured that there is no reason to believe that the information at issue was used by or will be disseminated by the criminal. Blackbaud also advised that it identified and eliminated the associated vulnerability that was at issue in this incident and hired its own cybersecurity team to continue monitoring for this type of criminal activity.

/ / /

Please let me know if you have questions or require any additional information.

Best regards,

SCHWABE, WILLIAMSON & WYATT, P.C.

/s/ Colin Folawn

Colin Folawn

CJF
Enclosure

PDX\125596\256665\CJF\28945392.1

YOUTHCARE

Dear XXXXX,

I hope this letter finds you and your loved ones safe and well during these challenging times.

I am writing to you today to let you know about a data security incident affecting our third-party data management provider, Blackbaud Inc., that involved some of your personal information. As you may be aware from your involvement in other community organizations, Blackbaud experienced a ransomware attack earlier this year. YouthCare has been focused on understanding the variable regulations in the home states where we have supporters in order to respond with the highest integrity. We wanted to be certain that our update to you was based on comprehensive review and facts.

YouthCare has worked with Blackbaud for seven years and initially hired them due to their national reputation and commitment to partnership in data management with their clients. We were truly unnerved and shocked when we were notified of this incident.

I have included details about the incident below and want to make sure you know that we have been assured that no credit card data, bank account information, or social security numbers were accessed in this incident.
I truly appreciate your support for youth experiencing homelessness in our community and apologize for the worry or inconvenience this might cause during this already difficult time. Please find more information about this incident below, as well as information about what you can do to protect your personal information.

What Happened?

On July 16, 2020, Blackbaud notified us of a data security incident, specifically a ransomware attack. In a ransomware attack, a criminal attempts to disrupt an organization by locking the organization out of its data and servers. Blackbaud has also informed us that its cyber security team, independent forensics experts, and law enforcement prevented the criminal from blocking system access and fully encrypting files and expelled the criminal from its system. Before being removed from the system, the criminal removed a copy of some data.
Blackbaud's explanation can be found at: https://www.blackbaud.com/securityincident.
Blackbaud has indicated that the incident occurred from February 7, 2020, through May 20, 2020, affecting nonprofit organizations across the nation. Although system access and full encryption of the files was prevented by Blackbaud's cybersecurity team, a backup file containing personal information was removed.
Blackbaud has told us that it paid a ransom in exchange for confirmation from the criminal that any data that was accessed and copied has been destroyed. We have been assured that there is no reason to believe that your information was used by or will be disseminated by the criminal.

What information was involved?

The file might have contained information pertaining to your relationship to YouthCare, including your name, address, date of birth, contact information, email address, gender, spouse's name, giving history, participation in our efforts, demographic information, and other information that you have provided to us. However, Blackbaud has confirmed that the criminal did not access the following encrypted information:

- credit card information,
- social security numbers,
- bank account information, and
- usernames or passwords.

YouthCare does not store donor credit card numbers, social security numbers, or bank account information, so this information was never accessible to the criminal.

What else is being done?

Blackbaud has informed us that it:

- Paid the cybercriminal a ransom to ensure that the copy was destroyed;
- Has no reason to believe that any data was or will be misused, disseminated, or made public;
- Identified and eliminated the associated vulnerability that was at issue in this incident; and
- Hired its own cybersecurity team to continue monitoring for this type of criminal activity.

In addition, Blackbaud has promised to accelerate its efforts to further strengthen its security controls.

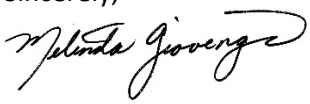
What can you do?

YouthCare hired and is working with ID Experts to ensure that you have professional support for any questions or actions you take. We encourage you to contact ID Experts with any questions by calling 1-833-755-1020. ID Experts are available Monday through Friday from 6:00 A.M.–6:00 P.M. Pacific Time. Again, at this time, there is no evidence that your information has been misused. Representatives of ID Experts have been fully versed on the incident, and they can answer questions or concerns that you might have regarding protection of your personal information.

In addition, please see the information from ID Experts on the pages that follow this letter.

As a supporter of YouthCare's work, you have placed your trust in us. We are doing everything in our power to honor your trust and ensure this does not happen again, while providing transparent information and comprehensive supports in the immediate. Again, if you have any questions or would like more information, please call 1-833-755-1020.

Sincerely,



Melinda Giovengo
CEO, YouthCare

MyIDCare

Recommended Steps to help Protect your Information

1. Telephone. Contact MyIDCare at 1-833-755-1020 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. 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.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069

www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

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.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that 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.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. 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.