MILLER NASH GRAHAM & DUNN LLP
ATTORNEYS AT LAW

Pier 70
2801 Alaskan Way, Suite 300
Seattle, Washington 98121

OFFICE 206.624.8300
FAX 206.340.9599

David L. Rice, P.C.
david.rice@millernash.com
206.777.7424 direct line

August 12, 2020

VIA E-MAIL (securitybreach@atg.wa.gov)

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Subject: Notice of Data Security Incident

Dear Attorney General Ferguson:

We are writing on behalf of our client, Mt. Baker Planned Parenthood ("MBPP"), to notify you of a security incident involving a service provider engaged by MBPP, which involved the disclosure of personal information of Washington residents.

1. Nature of the Incident

The service provider, Blackbaud, is one of the largest donor management software companies serving non-profits, including MBPP. Blackbaud notified MBPP on July 16, 2020 that it experienced a data breach between February 7, 2020 and May 20, 2020. This breach affected numerous non-profits like MBPP nationally and internationally. As part of the breach, the cybercriminal accessed a backup file that contained personal information of Washington residents that MBPP had uploaded to the Blackbaud service.

2. Number of Affected Washington Residents and Types of Compromised Personal Information

MBPP determined that the accessed file included personal information of 2,367 Washington residents. The personal information involved included the Washington resident's names, addresses, phone numbers, email addresses, and dates of birth.

Blackbaud informed MBPP that it engaged forensic experts and law enforcement to assist in the investigation and containment of the breach. Blackbaud also informed MBPP that

it believes the cybercriminal destroyed the personal information and that Blackbaud has no reason to believe that the data will be misused further or that the cybercriminal shared the data before destroying it.

3. Actions MBPP Is Taking

MBPP is now notifying the Washington residents whose personal information was compromised via the enclosed letter regarding the incident and providing them with steps to take to further protect their information. MBPP will complete mailing of the notifications by August 15, 2020.

Although the breach involved Blackbaud's network, not the network of MBPP, MBPP has taken this opportunity to review security protocols with its staff.

For further information or if you have any questions regarding this notice, please contact me at (206) 777-7427 or by email at david.rice@millernash.com.

Sincerely,

David L. Rice, P.C.

Enclosure

Planned Parenthood®
Care. No matter what.
Mt. Baker Planned Parenthood

<<First Name>> <<Last Name>>
<<Address 1>>
<<City>>,<<State>> <<Zipcode>>

Dear <<Salutation>>,

We are writing today to share information about a data security incident that may have involved your personal information.

A software service provider engaged by Mt. Baker Planned Parenthood (MBPP) experienced a data breach that affected numerous non-profits nationally and internationally, including MBPP. To be clear, *this was a breach of the software provider's network, not the network of MBPP.* As part of that incident, we understand that the cybercriminal may have accessed some of your personal information, ***although this did not include sensitive information, such as social security numbers, credit card data, or financial account information.***

MBPP is notifying you so that you are aware of this situation, understand what we are doing in response, and are aware of the resources that can help you if you have questions. We take your privacy seriously and value your trust, so please review this communication and let us know if you have any questions.

WHAT HAPPENED

The service provider, Blackbaud, is one of the largest donor management software companies serving non-profits, including MBPP. Blackbaud notified MBPP on July 16, 2020 that it experienced a data breach between February 7, 2020 and May 20, 2020. Blackbaud informed MBPP that as part of the breach the cybercriminal accessed a backup file that we believe contained some of your personal information listed below that Blackbaud obtained from MBPP in connection with the service.

Blackbaud informed MBPP that the cybercriminal destroyed the data. Blackbaud says that based on the results of its investigation and that of forensic experts and law enforcement, it is highly unlikely that the information was misused. Further, Blackbaud has no reason to believe that the data will be misused further or that the cybercriminal shared the data before destroying it.

(Over, please)

WHAT INFORMATION WAS INVOLVED

We understand that the file accessed by the cybercriminal may have contained the following personal information about you:

- Your name;
- Street address;
- Phone number;
- Email address; and
- Birth date.

WHAT MBPP IS DOING

We are deeply committed to the privacy of our supporters and have been working diligently since we were notified to obtain accurate information to share with you. MBPP continues to gather information about the incident and is taking additional steps to protect your data. We are conducting a close investigation to understand what measures Blackbaud is taking to remedy this situation and prevent further incidents.

Although we are not certain that the cybercriminal accessed your information in particular, we are contacting you to explain what happened and to provide you with steps you may wish to take to protect your personal information.

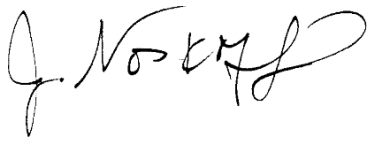
WHAT YOU CAN DO

Please review the attachment to this letter ("Steps You Can Take to Further Protect Your Information") for further information on actions you can take to protect yourself.

FOR MORE INFORMATION

If you'd like to discuss further, please contact me directly at 360.603.7703 or jnoskoff@mbpp.org.

Sincerely,



Jennie Noskoff
Director of Development

P/S You may receive more than one notification of this incident as each affiliate in WA State will send communication about the breach to its affected donors and in order to remain in compliance with state law. If this is YOU, thank you for supporting us all!

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

(Over, please)

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

You can contact the three credit reporting agencies listed above (Equifax, Experian and TransUnion) to request a security freeze. The credit reporting agencies' websites explain how to request a security freeze. *You must separately place a security freeze on your credit file with each credit reporting agency.*

To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.