September 28, 2020 via email

Washington State Attorney General's Office 1125 Washington St SE
PO Box 40100
Olympia, WA 98504 Security.breach@atg.wa.gov

RE: Notification of Data Security Event / Mary's Place Seattle

Dear Attorney General:

We are writing to let you know that Blackbaud, a Mary's Place vendor that manages our donor database, was recently the subject of a data security event. In July 2020, we learned that Blackbaud discovered and stopped a ransomware attack that occurred in May of this year. We understand that the cybercriminal removed a backup copy of donor information as part of a wide-reaching security event that involved data from multiple nonprofit organizations and other entities accepting donations. This backup copy contained the personal information of certain Washington residents.

The affected file included donation information, such as names of donors, contact information, dates of birth, and donation dates and amounts. We have identified personal information—dates of birth—for approximately 10,000 Washington residents. The cybercriminal did not access any credit card information, bank account information, or Social Security numbers, since we do not store this information in the database. Blackbaud also received confirmation that the copy of the data obtained by the cybercriminals was destroyed. We have no indication that these events resulted in any misuse of personal information.

We began notifying the above-mentioned Washington State residents via letter and/or email on September 28, 2020. We have attached a sample copy of the notification we are sending. We have been informed that Blackbaud has a number of safeguards in place and has already taken steps to enhance its systems to further protect against this kind of exploit. In particular, Blackbaud has accelerated efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint monitoring, and network-based platforms.

If your office requires any further information in this matter, please contact me at (206) 334-4687 or linda@marysplaceseattle.org.

Sincerely,

Linda Mitchell
Chief Communications Officer
Mary's Place

Dear donor,

We hope you and your family are healthy and well in these uncertain times. We are writing to provide you with information regarding a data security incident at an outside vendor, Blackbaud.

Blackbaud is one of the world's largest providers of fundraising management systems, serving more than 35,000 clients around the world in the nonprofit and education sectors, including Mary's Place. Blackbaud has informed us that they were the victim of a ransomware attack where a cybercriminal was able to remove a copy of certain backup data from many of their clients, including a subset of Mary's Place data. Our records indicate that this may have impacted some of your personal information, **but not your credit card, bank account, or Social Security number**.

We take the protection and proper use of your information very seriously. We are contacting you as a precautionary measure to share what Blackbaud has told its customers – including Mary's Place and many other nonprofit organizations—about the incident.

What Happened

In July 2020, Blackbaud notified Mary's Place that it had discovered and stopped a ransomware attack that occurred in May of this year. This was a wide-reaching security event that involved data from multiple nonprofit organizations and other entities accepting donations. We understand the cybercriminal removed a backup copy of donor information that Blackbaud maintained for us. This backup copy may have contained some of your personal information. Blackbaud reports that, after discovering the attack, their Cyber Security team — together with independent forensics experts and law enforcement — successfully prevented the cybercriminal from encrypting the data maintained by Blackbaud. According to Blackbaud, the company paid a demand for confirmation that the removed data was permanently destroyed.

For more information about this data security event, Blackbaud released a public statement acknowledging this incident and describing its cybersecurity practices, located at www.blackbaud.com/securityincident.

What Information Was Involved

The affected file contained donation information, such as names of donors, contact information, dates of birth, and donation dates and amounts. The cybercriminal **did NOT access any credit card information, bank account information, or Social Security numbers.**

Blackbaud also received confirmation that the copy of the data obtained by the cybercriminal was destroyed. We have no indication that these events resulted in any misuse of your personal information, but are notifying you so you can take certain precautions.

What We Are Doing

We take data security very seriously, especially as it relates to personal information. We deeply regret that this situation occurred. Once we were informed of the situation, we reviewed our security protocols and procedures to reduce the risk of this situation arising again in the future. We then reviewed the files to determine who may have been impacted, to allow us to communicate clearly

and accurately with those individuals and notify them of what happened. Blackbaud advised us that it implemented several changes to enhance the protection of personal information moving forward. In particular, Blackbaud has accelerated efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint monitoring, and network-based platforms.

We remain in regular contact with Blackbaud regarding the details of this incident, and we continue to monitor their response.

Again, we sincerely regret any concern this matter may cause. We are so grateful for your continued support and engagement.

Sincerely,

Marty Hartman
Executive Director

While we are confident that no sensitive financial information was exposed in the Blackbaud breach, it is always good practice to monitor your credit to guard against identity theft.

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission. U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

Equifax Information Services LLC
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com

Experian Credit Fraud Center P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000 1-800-680-7289 www.transunion.com