Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097

+1 206 839 4300
orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

August 14, 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 / ShelterBox

Dear Attorney General:

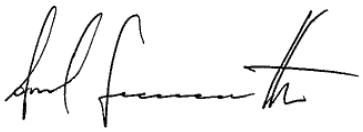
We are writing on behalf of ShelterBox USA, a not-for-profit organization, which was recently informed by Blackbaud, a leading software company ShelterBox uses to manage its donor databases, that it was recently the subject of a data security event. In July 2020, we learned that Blackbaud discovered 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 involving 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, including names of donors, contact information, dates of birth, and other donor information. We have identified personal information—dates of birth—for 778 Washington residents. 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 Washington State residents via letter on August 14, 2020 and have attached a sample copy of this notification. We have also 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) 839-4340 or aswaminathan@orrick.com.

Sincerely,



Aravind Swaminathan
Partner
Global Co-Chair Cyber, Privacy & Data Innovation

ShelterBox

August 14, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to let you know that Blackbaud, a leading software company that ShelterBox uses to manage our donor database, was recently the subject of a data security event. Our records indicate that this may have impacted some of your personal information. This letter outlines what happened and provides you with some steps you can take to help protect yourself.

What Happened

In July 2020, Blackbaud notified ShelterBox 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. According to Blackbaud, 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. 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, including names of donors, contact information, dates of birth, and other donor information. Blackbaud paid the ransom demand, and received confirmation from the attacker that he/she destroyed the copy of the data obtained in the attack. We have no evidence that personal information impacted by these events has been misused, but are notifying and providing information to you about precautions you can take.

What We Are Doing

We take data security seriously and deeply regret that this situation occurred. Once we were informed of the situation, we immediately reviewed our data management practices and 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.

What You Can Do

We encourage you to consider taking the following precautions:

- We urge you to remain vigilant against threats of identity theft or fraud. Regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. Report any unauthorized activity on your credit or banking accounts to your credit or banking providers immediately.
- Be alert for “phishing” emails from someone who acts like they know you and requests sensitive information over email, such as passwords, Social Security numbers or bank account information.
- It is always a best practice to change your financial account passwords often.
- If you suspect you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement.

- You may contact the FTC or your state attorney general to learn more about protecting yourself against identity theft. Attachment A, titled “Additional Information to Help Protect Yourself,” has more information about steps you can take to help protect yourself against identity theft or fraud.

For More Information

For more information about this matter, or if you have additional questions or concerns, you may contact the call center set up by ShelterBox at 1-877-514-0869 between the hours of 6:00 a.m. to 3:30 p.m. Pacific Time, Monday through Friday. Again, we sincerely regret any concern this matter may cause.

Sincerely,

Sarah Robinson
Senior Director of Fundraising, ShelterBox USA

Attachment

Attachment A

Additional Information to Help Protect Yourself

To help 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. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

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) 726-1014.

If you are concerned about identity theft, you might consider placing a security freeze on your report. To learn more about security freezes, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 105069	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
(888) 836-6351	(888) 397-3742	(800) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

You may obtain information about preventing identity theft at atg.wa.gov/identity-theftprivacy. You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Ave. NW, Washington, DC 20580; telephone (202) 326-2222; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general or the FTC.

North Dakota Residents: You may obtain information about preventing identity theft at https://attorneygeneral.nd.gov/consumer-resources/identity-theft/reporting-identity-theft.

Washington Residents: You may obtain information about preventing identity theft at atg.wa.gov/identity-theftprivacy.