## Appendix

On July 16, 2020, Blackbaud notified the BSA that Blackbaud had discovered an attempted ransomware attack on its systems. Blackbaud indicated to the BSA that the incident began on February 7, 2020 and possibly continued intermittently until May 20, 2020. According to Blackbaud, the attack was successfully stopped, and the cybercriminals were expelled from its systems. However, Blackbaud informed the BSA that the cybercriminals removed a copy of a backup file that it stored as part of its ordinary course of operations.

Upon learning of the incident from Blackbaud, the BSA conducted its own investigation of the Blackbaud services the BSA uses and the information provided by Blackbaud to determine what information was involved in the incident and identify the individuals whose information may be involved. The BSA determined the backup contained an unencrypted notation or media file that included the personal information of one Maine resident, including the individual's name and financial account number. Blackbaud advised that, based on the nature of the incident, their research, and law enforcement's investigation, the stolen data has been destroyed and there is no reason to believe any data went beyond the cybercriminals, was or will be misused, or will be disseminated or otherwise made available publicly.

On November 25, 2020, the BSA mailed a notification letter to the Maine resident via U.S.P.S. First-Class mail in accordance with Me. Rev. Stat. Tit. 10, §1348. A copy of the notification letter is attached. The BSA has also recommended that the notified resident be vigilant for indications of fraud or identity theft by reviewing their account statements and credit reports for any unauthorized activity. The BSA has provided a dedicated phone number where notified individuals may obtain more information regarding the incident.

Blackbaud has already implemented changes to its security controls to better protect against a potential future attack, and the BSA is working with Blackbaud and other resources to assess the best path forward. While the BSA was not the target of this attack, nor was it the only organization affected, it is reviewing its own security practices and system configurations to help better protect the information in its possession.

Boy Scouts of America
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

BOY SCOUTS OF AMERICA®

[redacted]

November 25, 2020

Dear [redacted],

As the Boy Scouts of America previously announced on July 29, 2020, our organization was one of many notified of a data security incident involving Blackbaud, one of the world's largest providers of customer relationship management software that we use at the national and council levels. We are writing to provide you additional information regarding the incident.

**What Happened?**
Blackbaud representatives notified the BSA on July 16, 2020, that its systems had been the target of a ransomware attack. Blackbaud indicated to us that the incident began on February 7, 2020 and possibly continued intermittently until May 20, 2020. According to Blackbaud, the attack was successfully stopped, and the cybercriminals were expelled from its systems. However, Blackbaud informed us that the cybercriminals removed a copy of a backup file that it stored as part of its ordinary course of operations.

Upon learning of the incident from Blackbaud, the BSA conducted its own investigation of the Blackbaud services the BSA uses and the information provided by Blackbaud to determine what information was involved in the incident and identify the individuals who might be affected. We determined that the backup file contained certain information pertaining to you.

**What Information Was Involved?**
The backup contained an unencrypted notation or media file that included your name and financial account number ending in 8313. Blackbaud advised us that, based on the nature of the incident, their research, and law enforcement's investigation, the stolen data has been destroyed and there is no reason to believe any data went beyond the cybercriminals, was or will be misused, or will be disseminated or otherwise made available publicly.

**What You Can Do.**
Out of an abundance of caution, we remind you it is always advisable to be vigilant for indications of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity. For some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

**What We Are Doing.**
We value your relationship with the BSA and the faith you put in us. Please know that we take the security of your information very seriously and share your concern about this incident. Blackbaud has already implemented changes to its security controls to better protect against a potential future attack, and we are working with Blackbaud and other resources to assess the best path forward. While the BSA was not the target of this attack, nor was it the only organization affected, we are reviewing our own security practices and system configurations to help better protect the information in our possession.

If you have any questions, please call 800-511-4722 from Monday through Friday between the hours of 8am-5pm Central Time.

Thank you for your continued support of Scouting.

Yours in Scouting,

Vijay Challa
Chief Technology Officer

**ADDITIONAL STEPS YOU CAN TAKE**

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

## Fraud Alerts and Credit or Security Freezes:

***Fraud Alerts:*** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

***Credit or Security Freezes:*** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

## Additional information for residents of the following states:

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov