BakerHostetler

Baker&Hostetler LLP
Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

August 21, 2020

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: Incident Notification

Dear Sir or Madam:

I am writing on behalf of my client, the Boy Scouts of America ("BSA") to notify you of a data security incident involving one of the BSA's third-party service providers, Blackbaud, Inc.

On July 16, 2020, Blackbaud notified the BSA that Blackbaud had discovered an attempted ransomware attack on its systems that occurred between February 7 and May 20, 2020. After discovering the attack, Blackbaud conducted an investigation and determined that the unauthorized individual removed a copy of a backup file that contained information relating to BSA's constituents.[1] The BSA was one of many organizations affected by this incident.

Upon receiving the notice from Blackbaud, the BSA conducted its own investigation and determined on July 21, 2020, that the stolen backup file contained information about approximately 981,068 Washington residents, potentially including their names and dates of birth. On August 21, 2020, the BSA began notification of the Washington residents via media notice, conspicuous posting on its website, and email notification to individuals with known email addresses in accordance with Wash. Rev. Code. § 19.255.010. Copies of the media, website, and email notification are enclosed. The BSA has established a dedicated point of contact where all individuals may obtain more information regarding the incident.

Blackbaud has assured the BSA that, as part of their ongoing efforts to better protect against an incident such as this, they have already implemented several changes that will protect data from

[1] Following the initial notice from Blackbaud, the BSA sent a courtesy communication to all the individuals in the database for whom it maintained an email address.

any subsequent incidents. First, Blackbaud informed the BSA that its teams were able to identify the vulnerability associated with this incident and were able to fix it. Additionally, Blackbaud informed the BSA that it is undertaking efforts to harden its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

David E. Kitchen
Partner

Enclosures

TO: All available emails for individuals in North Dakota and Washington State
SUBJECT: Additional Notice Regarding BSA Member, Donor, Alumni Data Impacted by Blackbaud Data Security Incident

I previously wrote to inform you of a data security incident involving Blackbaud, one of the world's largest providers of customer relationship management software and a third-party service provider for the Boy Scouts of America. I am writing again to provide you additional information regarding the incident.

Blackbaud representatives notified the BSA on July 16, 2020, that its systems had been the target of a ransomware attack. Blackbaud reported that the data security incident started on February 7, 2020 and possibly continued intermittently until May 20, 2020. The BSA was one of numerous organizations that were impacted.

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. We believe that file may have contained a limited amount of your information, including your name, contact information, date of birth, limited demographic data and a history of your relationship with the BSA.

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.

Nevertheless, out of an abundance of caution, 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

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 taking time to learn from this third-party incident and to review our own security practices and system configurations to better protect your information. Individuals with questions can contact our Blackbaud Response Center at IT@scouting.org.

Thank you for your continued support of Scouting.

Yours in Scouting,
Vijay Challa

BSA – Website Notification

The Boy Scouts of America values its relationships with members, alumni and donors and the faith they put in the BSA, and we are continuing our efforts to make sure our community is aware of a data security incident involving Blackbaud, one of the Boy Scouts of America's third-party service providers, and one of the world's largest providers of customer relationship management software.

Blackbaud representatives notified the BSA on July 16, 2020, that Blackbaud had been the target of a ransomware attack. Blackbaud reported that the data security incident started on February 7, 2020 and possibly continued intermittently until May 20, 2020. The BSA was one of numerous organizations that were impacted.

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. That file may have contained a limited amount of some information about individuals affiliated with the BSA, including names, contact information, dates of birth, limited demographic data and a history of their relationship with the BSA.

Blackbaud advised the BSA 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.

Nevertheless, out of an abundance of caution, the BSA reminds 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

Please know that the BSA takes the security of your information very seriously and shares your concern about this 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 taking time to learn from this third-party incident and to review its own security practices and system configurations to better protect your information. Individuals with questions can contact our Blackbaud Response Center at IT@scouting.org.

Thank you for your continued support of Scouting.

Media Contact:
PR@scouting.org

Boy Scouts of America Notifies Members, Donors and Alumni About Impact of Blackbaud Data Security Incident

Irving, TX – August 19, 2020 – The Boy Scouts of America ("BSA") is continuing efforts to notify members, donors, and alumni whose information may have been impacted by a recent security incident involving Blackbaud, a third-party provider of customer relationship management software used by the BSA. The organization first updated those whose information may have been impacted last month.

Blackbaud representatives notified the BSA on July 16, 2020, that its systems had been the target of a ransomware attack. Blackbaud reported that the data security incident started on February 7, 2020 and possibly continued intermittently until May 20, 2020. The BSA was one of numerous organizations that were impacted. 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. That file may have contained a limited amount of some information about individuals affiliated with the BSA, including names, contact information, dates of birth, limited demographic data and a history of their relationship with the BSA.

Blackbaud advised the BSA 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. Nevertheless, out of an abundance of caution, the BSA posted a notification of the incident on its website and sent notifications directly to some individuals. The BSA has also established a dedicated response team to answer questions that individuals may have about the incident. Individuals with questions can contact the BSA's Blackbaud Response Center at IT@scouting.org.

The BSA is reminding notice recipients to be vigilant for incidents of fraud or identity theft by reviewing account statements and free credit reports for unauthorized activity. 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.

For more information, please visit www.scouting.org/blackbaud-data-incident