CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

CAROLYN PURWIN RYAN
cpurwin@c-wlaw.com

Admitted in PA and NJ

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

August 21, 2020

Via Email (securitybreach@atg.wa.gov)
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Blackbaud Security Incident Notification

To Whom It May Concern:

I serve as counsel for the National Parks Conservation Association ("NPCA"), and provide this notification to you of a recent data security incident suffered by Blackbaud, Inc. ("Blackbaud"), a provider of cloud-based data management services. On July 16, 2020, NPCA was notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. Blackbaud's systems that were affected by the attack included a database containing certain information about NPCA's donors. According to the notification provided by Blackbaud, the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud's database. Blackbaud informed us that it paid a ransom to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Notably, Blackbaud has assured the NPCA that no credit card information, bank account information, username and passwords, or Social Security numbers were impacted as a result of this incident. As Blackbaud provided only general information regarding the scope of the incident, NPCA immediately began an internal investigation. As a result of the internal investigation, NPCA has discovered that date of birth information was present within the database and not encrypted by Blackbaud. NPCA has learned that the potentially impacted data included information relating to 12,640 Washington residents.

While we believe the information potentially impacted, including the circumstances of the incident, provide little to no risk of harm to the affected individuals, the NPCA will be promptly notifying the affected individuals on August 21, 2020. A copy of the drafted letter is attached. NPCA is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: Carolyn Ryan
Carolyn Purwin Ryan

<<First Name>> <<Last Name >>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>> <<Date>>
<<Country>>

RE: Blackbaud Data Security Notification

Dear <<First Name>> <<Last Name >>,

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 NPCA. Blackbaud recently informed us that they had been 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 NPCA data. NPCA takes 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 about the incident.

What Happened

NPCA was recently notified by Blackbaud, one of NPCA's third-party service providers, of a security incident. According to Blackbaud's communication, there was an attempted ransomware incursion into their systems beginning on February 7, 2020 which continued until May 20, 2020. Prior to being locked out of Blackbaud's systems, the cybercriminal reportedly removed a copy of the backup files of some customers that may have contained 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.

What Information Was Involved

According to Blackbaud, **the potentially impacted data may have contained your contact information, date of birth, and a history of your relationship with NPCA, including a record of giving**. The cybercriminal **did not access credit card information, bank account information, or social security numbers**. Blackbaud has further stated that this information, if stored on Blackbaud systems, is secured using encryption technologies.

Based on the nature of the incident, their research, and third-party (including law enforcement) investigation, Blackbaud states that it has no reason to believe that any data went beyond the cybercriminal, was misused, or will be disseminated or otherwise made available publicly.

Blackbaud's Remediation Efforts

Blackbaud has hired a third-party security service to monitor for any improper use of this data indefinitely on a 24/7/365 basis. As part of its ongoing efforts to help prevent something like this from happening in the future, Blackbaud has affirmed to us that it has already implemented changes to protect its system from any subsequent incidents:

- Blackbaud has identified the vulnerability associated with this incident, including the tactics used by the cybercriminal, and have taken actions to fix it;

- Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. They are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms;
- Blackbaud is working to expand their use of encryption technologies to provide additional security.

We very much regret that the incident experienced by Blackbaud occurred. We remain in regular contact with Blackbaud regarding the details of this incident, and we continue to monitor their response. As a best practice, we recommend people remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities. While the potentially impacted information is very limited in scope, and while Blackbaud has assured us that all removed data has been destroyed, we have enclosed additional information regarding steps you can take to further secure your information should you feel such steps are necessary.

Please be assured that we take data protection very seriously and we are grateful for our community's continued support and engagement. If you have any immediate concerns or questions regarding this matter, please do not hesitate to contact us at 1-800-628-7275.

Sincerely,

Derrick Pressley
Chief Information Officer

ADDITIONAL ACTIONS YOU CAN TAKE TO FURTHER SECURE YOUR INFORMATION

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 6790	P.O. Box 1017	P.O. Box 105069
Fullerton, CA 92834	Allen, TX 75013	Atlanta, GA 30348
1-800-680-8289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.