



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

James Monagle
Office: (267) 930-1529
Fax: (267) 930-4771
Email: jmonagle@mullen.law

178 East Hanover Ave, #103-373
Cedar Knolls, NJ 07927-2013

November 5, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Green America located at 1612 K Street NW, Suite 600, Washington DC 20006, and are writing to notify your office of an incident that may affect the security of some personal information relating to one thousand one hundred twenty-seven (1,127) Washington residents. The investigation into this matter is ongoing, and this notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Green America does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was potentially exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Green America immediately commenced an investigation to determine what, if any, sensitive Green America data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. After receiving further information from Blackbaud, on or about September 16, 2020, Green America determined the information potentially affected may have contained personal information.

The information that could have been subject to unauthorized access includes name, address, and date of birth.

Notice to Washington Residents

On or about November 5, 2020, Green America provided written notice of this incident to all affected individuals, which includes one thousand one hundred twenty-seven (1,127) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Green America moved quickly to investigate and respond to the incident, assess the security of Green America systems, and notify potentially affected individuals. Green America is also working to implement additional safeguards and training to its employees. As part of Green America's ongoing commitment to the security of information in its care, Green America is working to review its existing policies and procedures regarding third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Green America is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Green America is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Green America is notifying other relevant state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1529.

Very truly yours,

A handwritten signature in black ink, appearing to read 'James Monagle', with a long horizontal flourish extending to the right.

James Monagle of
MULLEN COUGHLIN LLC

JZM/nfw
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 5, 2020

F9406-L01-0000001 P003 T00017 *****ALL FOR AADC 123



SAMPLE A SAMPLE
APT B
123 ANY ST
ANYTOWN, US 12345-6789



Dear Sample A Sample,

I hope this letter finds you well.

I want to thank you for your support of Green America and our work to make this a greener world. At Green America, it is individuals like you that make our work possible.

As a supporter of Green America, I'm writing to inform you that one of our third-party vendors, Blackbaud, Inc., which has a database that includes our donor information, was a victim of a ransomware attack.

Please know that Blackbaud has confirmed that certain categories of sensitive personal information such as social security numbers commonly targeted by cyber criminals was encrypted, and therefore NOT affected by this incident.

However, we are reaching out to you to let you know how this incident may have involved your other personal information.

Attached is a description of the incident, what Green America is doing next, and helpful tips for protecting your personal information that we encourage you to review. The tips are particularly important for all you do online in this day and age of cyberattacks. **If you have any questions or concerns about this incident or your rights, please refer to the contact information in the attached notice.**

If you have general membership questions, our member services team is here for you. Please contact us at Members@GreenAmerica.org or call 1.800.58.GREEN.

Thank you for all you do to protect people and the planet.

In Cooperation,

Dana Christianson
Director of Membership

0000001



F9406-L01



[Extra1]

Dear Sample A Sample:

Green America writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, Green America received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Green America. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Green America data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was apparently exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Green America immediately commenced an investigation to determine what, if any, sensitive Green America data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. After receiving further information from Blackbaud, on or about September 16, 2020, Green America determined the information potentially affected may have contained your personal information.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and [Extra2]. However, please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

What We Are Doing in Response? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying state and federal regulators, as required.

What Can You Do? We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 210-4612 Monday through Friday 6:00am – 8pm PST, and Saturday and Sunday 8:00am – 5:00pm PST. You may also write to Green America at 1612 K Street NW, Suite 600, Washington, DC 20006. Please reference **DB23488** when speaking with an agent.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink that reads "Dana Christianson".



STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

<https://www.transunion.com/fraud-alerts>

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

0000001





Additional Information

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.