17518

Dear [First Name][Last Name]:

Seeds of Peace is writing to notify you of an incident that may involve certain pieces of your personal information due to an incident at its database and relationship management services provider, Blackbaud. We take this incident very seriously and as a precaution, we are providing you with information and access to resources so that you can protect your information, should you feel it is appropriate to do so.

The confidentiality, privacy, and security of information is one of our highest priorities. We regret any inconvenience or concern this incident may cause. As an added precaution, Seeds of Peace is offering you access to 24 months of free credit monitoring and identity protection services through Kroll Inc.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

1. You must activate your identity monitoring services by **11/11/2020.** Your Activation Code will not work after this date.
2. Visit **https://enroll.idheadquarters.com/redeem** to activate your identity monitoring services. Provide Your Activation Code: **[Activation Code]** and Your Verification ID: [redacted]
3. To sign in to your account after you have activated your identity monitoring services, please visit **https://login.idheadquarters.com/**

If you have questions, please call (866) 925-2006 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

1 - Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

We encourage you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-	www.equifax.com/personal/credit-report-services

resource/place-fraud-alert

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

We understand you may have questions that are not answered in this letter. If you have questions or concerns regarding this incident, please call (866) 925-2006 Monday through Friday from 9:00 a.m. to 6:30 or reply directly to this email.

Sincerely,

Jenna Markowitz
Legal and Business Affairs Director, Seeds of Peace

Lele Levay
Director of Advancement, Seeds of Peace

Marni Pearce
Director of Data and Development Operations, Seeds of Peace

EXHIBIT B

Dear [redacted],

Please see a personalized note below for your organization from our Chief Information Officer. Thank you.

Dear [redacted]

We are writing to notify you about a particular security incident that recently occurred. Please review this email for a personalized link, next steps and resources created for your organization specifically.

What Happened

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. At Blackbaud, our Cyber Security team successfully defends against millions of attacks each month and is constantly studying the landscape to ensure we are able to stay ahead of this sophisticated criminal industry. **In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.**

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud NetCommunity, Blackbaud Financial Edge NXT, and Blackbaud Raiser's Edge NXT backup was part of this incident. Again, the file the cybercriminal removed a copy of did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident.

And again, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any

data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

We have created a resource page for you at www.blackbaud.com/incidentresources that features a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars (hosted by Rich Friedberg, Blackbaud's Chief Information Security Officer and Cameron Stoll, our Head of Privacy), information about our future plans, and other resources.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in your toolkit to make it easier.

To ensure all your questions are answered as quickly as possible, we encourage you to first review the resources we provided at the link above. If you still have questions after reviewing these resources, we are here to help. Please contact the dedicated team we have established for this incident:

- **North and South America:** 1-855-907-2099 between 9 a.m. and 9 p.m. ET Monday – Friday

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. We apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

Sincerely,

Todd Lant
Chief Information Officer

blackbaud

EXHIBIT C

Seeds of Peace, and many other nonprofit organizations and educational institutions, rely on a software provider called Blackbaud for database and relationship management services. On July 16, 2020, Blackbaud informed us that between February and May 2020, they experienced a data security incident that resulted in the unauthorized acquisition of data impacting a large group of the organizations to whom they provide services, including Seeds of Peace.

What Information Was Involved?

Based on our ongoing investigation, the Seeds of Peace information impacted involved backup files that may have contained names, a limited number of Social Security Numbers, dates of birth, passport numbers, contact information, demographic information, and donation histories. **Blackbaud has assured us that the attacker did not gain access to any bank account or credit card information.**

What We Are Doing?

Promptly after Blackbaud notified us of this incident, we took steps to determine its nature and scope, including whether any personal information was impacted. **Blackbaud has indicated to us that, based on its investigation, they do not believe that any Seeds of Peace data has been misused or will be disseminated or otherwise made publicly available.** We continue to investigate this incident and are coordinating closely with Blackbaud to monitor the situation. Blackbaud also has engaged third-party experts to actively monitor for suspicious activity and has not at this time identified any evidence that the Seeds of Peace data has been misused. In addition, Blackbaud has stated that it has implemented additional measures and safeguards to prevent this type of attack from happening again.

What Can You Do?

We take our obligation to safeguard personal information very seriously and are alerting those affected about this incident so they can take steps to help protect themselves. Steps they can take include the following:

· *Register for Credit Monitoring Services.* We have arranged to offer identity protection and credit monitoring services for two years at no cost for those with Social Security Numbers

and non-expired U.S. passport numbers who are impacted. If you think you may have had this type of information compromised, please reach out to us at marni@seedsofpeace.org.

· *Order a Credit Report.* Those impacted are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage those impacted to remain vigilant by reviewing their account statements and monitoring their free credit reports.

· *Review the Reference Guide below.* The Reference Guide provides information on registration and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We take the security of personal information very seriously. We hope this information and the attached Reference Guide are useful. If you have any questions regarding this incident, please email Marni Pearce at marni@seedsofpeace.org.

Sincerely,

Jenna Markowitz
Legal and Business Affairs Director, Seeds of Peace

Lele Levay
Director of Advancement, Seeds of Peace

Marni Pearce
Director of Data and Development Operations, Seeds of Peace

REFERENCE GUIDE

We encourage affected individuals to take the following steps:

Order Your Free Credit Report

To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report

Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents

If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

· Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.

· File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Information Services LLC
P.O. Box 740241 Atlanta, GA 30374
1-800-525-6285 www.equifax.com

Experian Inc.
P.O. Box 9554 Allen, TX 75013
1-888-397-3742 www.experian.com

TransUnion LLC
P.O. Box 2000 Chester, PA 19016
1-800-680-7289 www.transunion.com

Consider Placing a Security Freeze on Your Credit File

You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

· Your full name with middle initial and generation (such as Jr., Sr., II, III)

· Your Social Security Number

· Your date of birth

· Addresses where you have lived over the past five years

· A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

· Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents

You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202

(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico residents

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York Residents

You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341

1-800-771-7755 (toll-free)

1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005

Phone: (212) 416-8433
https://ag.ny.gov/internet/resource-center

For North Carolina Residents

You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001

(877) 566-7226 (toll-free in North Carolina)

(919) 716-6400
www.ncdoj.gov

For Rhode Island Residents

You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

(401)-274-4400
http://www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account. There is one Rhode Island resident impacted by this incident.

For Washington, D.C. Residents

You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW

Suite 1100 South
Washington, D.C. 20001

(202)-727-3400
https://oag.dc.gov