



Allen E. Sattler  
Phoenix Plaza Tower II  
2929 North Central Avenue, Suite 1700  
Phoenix, Arizona 85012-2761  
Allen.Sattler@lewisbrisbois.com  
Direct: 714.668.5572

September 30, 2020

**VIA E-MAIL**

Attorney General Bob Ferguson  
Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100  
E-Mail: [SecurityBreach@atg.wa.gov](mailto:SecurityBreach@atg.wa.gov)

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent World Relief, a global Christian humanitarian organization based in Baltimore, Maryland. The purpose of this letter is to notify you that World Relief was recently informed that one of its vendors, Blackbaud, Inc. ("Blackbaud"), experienced a data security incident that may have involved personal information related to World Relief's constituents. World Relief takes the protection of all information within its control very seriously and is working with Blackbaud to prevent a similar incident from occurring in the future.

**1. Nature of the Security Incident.**

On July 16, 2020, Blackbaud reported to World Relief that Blackbaud had experienced a data security incident that may have involved unauthorized access to World Relief data. Upon learning this information, World Relief immediately launched its own investigation, which included requesting information from Blackbaud about the incident, data involved, and the findings of Blackbaud's forensics investigation. According to Blackbaud, the unauthorized access may have occurred between February 7, 2020 and May 20, 2020. On September 8, 2020, World Relief finished its review of its impacted databases, and this review revealed that a select number of its constituents' dates of birth were contained therein, and thus could have been accessed without authorization as a result of the incident.

**2. Number of Washington Residents Affected.**

World Relief notified 734 residents of Washington via written letter on September 28, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

### 3. Steps Taken Relating to the Incident.

Upon learning of the incident, World Relief immediately launched an independent investigation and worked with Blackbaud to ensure that its data was secure. Blackbaud confirmed that the matter had been reported to law enforcement and that the Federal Bureau of Investigation (FBI) was actively involved in the investigation. Blackbaud also reported that it has no reason to believe that any data was or will be misused. Blackbaud further advised that it had not detected any information relating to the incident through its continuous dark web monitoring activities.

Furthermore, World Relief has notified the potentially-affected individuals and provided guidance on steps that can be taken to further protect the individuals' personal information (see attached sample consumer notification letter).

### 4. Contact Information.

World Relief remains dedicated to protecting the personal information of its constituents. Please do not hesitate to contact me should you have any questions.

Very truly yours,



Allen E. Sattler of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES

cc: Jenna Disser, Lewis Brisbois

Enclosure: Consumer Notification Letter (Sample)



C/O ID Experts  
10300 SW Greenburg Rd., Suite 570  
Portland, OR 97223

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

September 28, 2020

Re: Notice of Data Security Incident

Dear <<Name>>,

We are writing to notify you of a data security incident experienced by Blackbaud, Inc. (“Blackbaud”), a third-party vendor which provides donor management software services to World Relief. Our investigation recently determined that a limited amount of your information could have been involved in the incident. **World Relief treats your privacy and security with the utmost care, and the only personal information potentially involved was your name and date of birth.** That said, keep reading for more information regarding the incident and the steps that can be taken to help protect your information.

**What Information Was Involved?** The only personal information contained within the affected file was limited to your name and date of birth.

**What Happened?** In July 2020, World Relief was notified by Blackbaud, a large provider of cloud-based data management services to World Relief and many other not-for-profit organizations, that Blackbaud had discovered and stopped a ransomware attack that occurred in May 2020. According to Blackbaud, unauthorized individuals may have accessed information in certain databases between February 7, 2020 and May 20, 2020. Upon learning this information, we immediately launched an internal investigation. We’ve since confirmed that much of the information in the databases was protected by encryption, and therefore inaccessible to the unauthorized individuals. However, Blackbaud indicated that the unauthorized individuals may have had access to a select number of backup files, which may have included information pertaining to World Relief and its constituents.

As such, World Relief worked diligently to ascertain whether any of its donors’ information was stored in its Blackbaud software. World Relief ultimately determined that a limited amount of your personal information was amongst the unencrypted data stored in the software. Blackbaud has informed us that they have no reason to believe that any data has or will be misused, or that any data will be shared publicly.

Furthermore, Blackbaud has confirmed that payment card information, Social Security numbers, and financial account information contained in the affected systems were encrypted and the decryption keys were not compromised. And regardless, World Relief does not request or store any of its constituents’ Social Security numbers in its data systems. Therefore, the unauthorized individuals did not access or acquire any payment card information, Social Security numbers, or financial account numbers as a result of this incident.

**What Are We Doing at World Relief?** In addition to the steps outlined above, we conducted our own investigation and worked with Blackbaud to ensure that our data is now secure. We also received confirmation that Blackbaud had reported this incident to the Federal Bureau of Investigation. We will provide law enforcement with all cooperation needed to hold the perpetrators accountable.

Based on our investigation and correspondence with Blackbaud, we have no reason to believe that your data was, or will be, misused as a result of this incident. However, we are providing notification out of an abundance of caution.

**What You Can Do:** You can follow the standard recommendations included with this letter to further secure and protect your personal information.

**For More Information:** If you have any questions about this letter, please call 1-800-939-4170. We regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin Sanderson", written in a cursive style.

Kevin Sanderson  
Chief Administrative Officer

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

<b>TransUnion</b>	<b>Experian</b>	<b>Equifax</b>	<b>Free Annual Report</b>
P.O. Box 1000 Chester, PA 19016 1-800-916-8800 <a href="http://www.transunion.com">www.transunion.com</a>	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://annualcreditreport.com">annualcreditreport.com</a>

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

<b>Federal Trade Commission</b>	<b>Maryland Attorney General</b>	<b>North Carolina Attorney General</b>	<b>Rhode Island Attorney General</b>
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a> 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 <a href="http://oag.state.md.us">oag.state.md.us</a> 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 <a href="http://ncdoj.gov">ncdoj.gov</a> 1-877-566-7226	150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">http://www.riag.ri.gov</a> 401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**Personal Information of a Minor:** You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>.