[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: Woods, Jennifer <WoodsJe@gc.adventist.org>
Sent: Tuesday, September 29, 2020 12:25 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: Notification of personal data security incident involving New Hampshire residents

Dear Attorney General MacDonald,

I am writing on behalf of ADRA International to notify you of a security incident that occurred involving the personal information of up to 8 New Hampshire residents.

I am writing to let you know that ADRA International was notified of a data security incident at Blackbaud, a third-party vendor whose fundraising and donor engagement software is used by more than 25,000 nonprofit organizations worldwide. In July 2020, we received notification from Blackbaud that they discovered a cyberattack on one of their systems that houses donor information. Unfortunately, ADRA was one of a number of organizations impacted by this security breach. A detailed explanation of the incident is available on Blackbaud's website at: blackbaud.com/securityincident.

The Blackbaud breach, discovered in May 2020, may have included personal data for some of our ADRA supporters including names, addresses, phone numbers, date of birth, giving history, credit card and bank account information. According to Blackbaud, based on the nature of the incident, their research, and third party (including law enforcement) investigation, they "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."

Blackbaud believes the risk to individuals whose data was accessed is very low. However, in an abundance of caution, Blackbaud has put in place dark web monitoring intended to detect trafficking of any of the copied data.

We are maintaining regular contact with Blackbaud and staying well-informed of any developments. We have reviewed our internal policies on data security and have made adjustments in light of what could have occurred—but did not.

Please contact me if you need any additional information regarding this incident.

Jennifer Woods
Legal Counsel
ADRA International

Adventist Development & Relief Agency
12501 Old Columbia Pike 1.800.424.ADRA (2372)
Silver Spring, MD 20904 ADRA.org

September 2020

John Doe
123 Main Street
Anytown, MD 20904

Dear John,

I am writing to let you know that ADRA International was notified of a data security incident at Blackbaud, a third-party vendor whose fundraising and donor engagement software is used by more than 25,000 nonprofit organizations worldwide. In July 2020, we received notification from Blackbaud that they discovered a cyberattack on one of their systems that houses donor information. Unfortunately, ADRA was one of a number of organizations impacted by this security breach. A detailed explanation of the incident is available on Blackbaud's website at: blackbaud.com/securityincident.

What Kind of Data Was Affected?
The Blackbaud breach, discovered in May 2020, may have included personal data for some of our ADRA supporters including names, addresses, phone numbers, date of birth, giving history, credit card and bank account information. According to Blackbaud, based on the nature of the incident, their research, and third party (including law enforcement) investigation, they "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."

Blackbaud's Response
Blackbaud believes the risk to individuals whose data was accessed is very low. However, in an abundance of caution, Blackbaud has put in place dark web monitoring intended to detect trafficking of any of the copied data.

ADRA's Response
Supporters like you trust us with your information, and we do not take this responsibility lightly. Please know that we here at ADRA are maintaining regular contact with Blackbaud and staying well-informed of any developments. We have reviewed our internal policies on data security and have made adjustments in light of what could have occurred—but did not.

Some of those adjustments we will not publish, but we are happy to discuss them with any donor who would like more assurance that we are doing our due diligence.

over, please

Talk to Us
We value your privacy and deeply regret that this incident occurred. If you have any immediate concerns or questions, please contact one of our team members at 1.800.424.ADRA (2372).

Thank you for your continued partnership with ADRA so that all may live as God intended. May God continue to bless you and those you love.

With deepest gratitude,

Michael Kruger
President, ADRA International

Steps You Can Take to Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, it is recommended 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

It is recommended that you 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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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.

- **Take Advantage of Additional Free Resources on Identity Theft**

It is recommended that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.