Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 21, 2020

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Heifer Project International ("Heifer International") located at 1 World Avenue, Little Rock, Arkansas 72202, and are writing to notify your office of an incident that may affect the security of some personal information relating to six thousand three hundred thirteen (6,313) Iowa residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Heifer International does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 16, 2020, Heifer International 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 Heifer. Upon receiving notice of the cyber incident, Heifer International immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Heifer International data. On or about July 22, 2020, Heifer received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information.

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 investigate. Following its investigation, Blackbaud notified

its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Heifer International immediately began to determine what, if any, sensitive Heifer International data was potentially involved.

Our investigation determined that the involved Blackbaud system contained personal information, including names, driver's license number, and financial account number.

Notice to Iowa Residents

On or about Friday, August 21, 2020 Heifer International provided written notice of this incident to all affected individuals, which includes six thousand three hundred thirteen (6,313) Iowa 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, Heifer International moved quickly to investigate and respond to the incident, assess the security of Heifer International systems, and notify potentially affected individuals. Heifer International is also working to implement additional safeguards and training to its employees.

Additionally, Heifer International 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. Heifer International is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB:mf1

Exhibit A

HEIFER INTERNATIONAL
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

I am writing to you today to inform you of a recent incident that may affect the privacy of some of your information. This letter provides information about what happened, our response, and resources available to you to help protect your information from possible misuse. Heifer International takes the privacy and security of your information very seriously and we sincerely apologize for any inconvenience this incident may cause.

What Happened? On Thursday, July 16, 2020, Heifer International received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a leader in cloud computing, and hosts customer relationship management databases for many nonprofits, including Heifer International. Upon receiving notice of the cyber incident, Heifer International immediately started an investigation to determine the nature and scope of the incident and any impact on its data.

Blackbaud reported to us that in May of 2020, Blackbaud discovered a ransomware incident during which an unknown actor attempted to disrupt business by locking companies out of their data. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified its customers that the unknown actor may have accessed or acquired certain Blackbaud customer data, before being locked out of the environment by Blackbaud in May of 2020.

What Information was Involved? Our investigation determined that the involved Blackbaud system contained your name and <<Breached Elements>>. Please note that, to date, we have not received any information from Blackbaud indicating that your information was specifically accessed or acquired by the unknown actor.

What we are Doing. Upon learning of the Blackbaud incident, Heifer International immediately began to determine what, if any, sensitive data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. Heifer International later received further information from Blackbaud that enabled us to determine the information affected may have contained personal information.

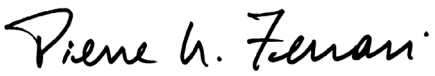
Heifer International is very careful about the information it stores and works hard to keep your personal information safe. We take the confidentiality, privacy, and security of information in our care extremely seriously. As part of our ongoing commitment to the security of information in our care, we took immediate steps to reduce risk, are reviewing the way we work with third-party vendors, and are working with Blackbaud to evaluate additional measures to protect against this type of incident in the future. We will also be notifying state regulators, as required.

What You Can Do. Please be especially cautious if you are contacted by anyone requesting personal information or payments at this time. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your 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 855-913-0601 between the hours of 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday, except holidays.

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

Sincerely,



Pierre U. Ferrari
President and Chief Executive Officer
Heifer International

(enclosure)

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, 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 **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 (5) 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 (7) 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 www.transunion.com/fraud-victim-resource/place-fraud-alert	**Equifax** P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

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); 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.

For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, 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. ***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 violators. 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*****,** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. ***For North Carolina residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. ***For Rhode Island residents***: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 1425 Rhode Island residents impacted by this incident. This notice has not been delayed by a law enforcement investigation. ***For District of Columbia residents:*** The District of Columbia Attorney General can be reached at: 441 4th St NW #1100, Washington, DC 20001, oag.dc.gov, (202) 727-3400.