



**American  
Heart  
Association.**

*Chairman of the Board*

Bertram L. Scott

*President*

Mitchell S. V. Elkind, MD, MS, FAHA

*Chairman-elect*

Raymond P. Vara, Jr.

*President-elect*

Donald M. Lloyd-Jones,  
MD, ScM, FAHA

*Immediate Past Chairman*

James J. Postl

*Immediate Past President*

Robert A. Harrington, MD, FAHA

*Treasurer*

Marsha Jones

*Directors*

Mary Ann Bauman, MD  
Regina M. Benjamin, MD, MBA  
Douglas S. Boyle  
Keith Churchwell, MD, FAHA  
Shawn A. Dennis  
Linda Gooden  
Ron W. Haddock  
Joseph Loscalzo, MD, PhD, FAHA  
Cheryl Pegus, MD, MPH  
Ileana Piña, MD, FAHA  
Marcella Roberts, Esq.  
Lee Schwamm, MD, FAHA  
Svati Shah, MD, MS, MHS, FAHA  
Lee Shapiro  
David A. Spina  
John J. Warner, MD, FAHA  
Thomas Pina Windsor  
Joseph C. Wu, MD, PhD, FAHA

*Chief Executive Officer*

Nancy A. Brown

*Chief Operating Officer*

Suzie Upton

*Chief Science and Medical Officer*

Mariell Jessup, MD, FAHA

*Chief Administrative Officer and*

*Corporate Secretary*

Larry D. Cannon

September 15, 2020

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: Notice of Security Incident involving the American Heart Association

Dear General Ferguson:

On behalf of the American Heart Association (“AHA”), I am writing to notify you of a recent security incident that affected the personal information of some Washington residents as a result of a security incident at a service provider. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including AHA. On July 16, 2020, Blackbaud notified AHA that it had discovered a ransomware attack on Blackbaud’s network in May 2020. Upon learning of the Blackbaud incident, AHA immediately began to determine what, if any, sensitive AHA data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. AHA confirmed that unencrypted dates of birth related to Washington residents were impacted on August 18, 2020.

Blackbaud reported that the unauthorized access to the system occurred sometime between February 7, 2020, and May 20, 2020, and According to Blackbaud, it conducted an investigation and determined that backup files containing information from some of its clients had been taken from its network sometime before Blackbaud locked the unknown actor out of its environment prior to May 20, 2020. Blackbaud paid a ransom and obtained a statement from the cybercriminal that the backup files that were removed from its network had been destroyed. Blackbaud reported that it has been working with law enforcement to further investigate this incident. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, and have implemented several changes to mitigate the risk of future attacks.

The Data Event

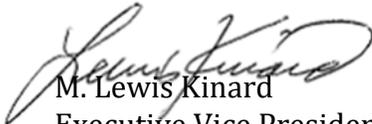
AHA has completed our investigation where we determined that the backup files exposed in the cyberattack contained the following personal information that could have been subject to unauthorized access: the individuals' names and full dates of birth. **AHA does not store credit card information, financial account information, social security numbers, or passwords in this database** and that information was, therefore, not compromised by this incident. Blackbaud stated that it has no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

Notice to Washington Residents

AHA will be providing written notice of this incident to all affected individuals for whom we have current addresses in the State of Washington, which includes 7,658 Washington residents. We expect this notice to be mailed on or about September 16, 2020. A copy of the form of notification letter that is being sent on behalf of AHA is attached.

If you have any questions, please do not hesitate to contact me.

Sincerely,



M. Lewis Kinard  
Executive Vice President, General Counsel & Assistant Corporate Secretary  
American Heart Association

Enclosure



*Chairman of the Board*

Bertram L. Scott

*President*

Mitchell S. V. Elkind, MD, MS, FAHA

*Chairman-elect*

Raymond P. Vara, Jr.

*President-elect*

Donald M. Lloyd-Jones,  
MD, ScM, FAHA

*Immediate Past Chairman*

James J. Postl

*Immediate Past President*

Robert A. Harrington, MD, FAHA

*Treasurer*

Marsha Jones

*Chief Executive Officer*

Nancy A. Brown

*Chief Operating Officer*

Suzie Upton

*Chief Science and Medical*

*Officer* Mariell Jessup, MD, FAHA

*Chief Administrative Officer and  
Corporate Secretary*

Larry D. Cannon

September 16, 2020

Dear [Salutation]:

We at the American Heart Association (AHA) want you, one of our supporters, to know we have addressed a data security issue. AHA, along with many other institutions and nonprofits, was recently notified that one of our technology partners experienced a data security incident that may have involved the information of a number of members of the AHA community. This notice explains the incident, measures we have taken, and additional steps you can take in response.

### *What Happened*

Blackbaud is a cloud-based software company that provides services to thousands of entities, such as schools, hospitals, and other non-profits, including AHA. On July 16, 2020, Blackbaud notified us that it had discovered an attack on Blackbaud's network in May 2020. The unauthorized access to the system occurred sometime between February 7, 2020, and May 20, 2020. Blackbaud reported that it conducted an investigation and determined that backup files containing information from some of its clients had been taken from its network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Blackbaud took steps to ensure that the cybercriminal destroyed the information that had been stolen and worked with law enforcement to investigate this incident.

### *What Information Was Involved*

We determined that the backup files may have contained some or all of the following personal information: demographic data such as your name and full date of birth, and contact information. AHA does not store credit card information, financial account information, social security numbers, or passwords in this database and that information was therefore not compromised by this incident.

### What We Are Doing

The security of your personal information is very important to the American Heart Association. Because of our care and concern for your privacy, we are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident and have implemented several changes that will better protect your data from any subsequent incidents. AHA remains in regular contact with Blackbaud regarding the details of this incident and we will continue to monitor their response.

### Additional Steps You Can Take

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. The FTC is a good resource and can be reached at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or by calling 1-877-IDTHEFT (1-877-438-4338). You may also mail them at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You can also contact the national credit reporting agencies at:

Equifax  
1-866-349-5191  
<http://www.equifax.com>  
P.O. Box 740241  
Atlanta, GA 30374

Experian  
1-888-397-3742  
<http://www.experian.com>  
P.O. Box 2002  
Allen, TX 75013

TransUnion  
1-800-888-4213  
<http://www.transunion.com>  
P.O. Box 2000  
Chester, PA 19016

### For More Information

AHA takes the protection and proper use of your information very seriously. We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us at [jill.dotts@heart.org](mailto:jill.dotts@heart.org).

Sincerely,

American Heart Association